CSRA
A General Dynamics Information Technology company

North Carolina Department of Health and Human Services (NC DHHS)

Division of Health Benefits (DHB)
Division of Mental Health (DMH)
Division of Public Health (DPH)

Standard Companion Guide Trading Partner Information Instructions related to Transactions based on ASC X12 Implementation Guides, version 005010, for MMIS NCTracks starting July 1, 2013

NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

Disclosure

This template is Copyright © 2010 by The Workgroup for Electronic Data Interchange (WEDI) and the Data Interchange Standards Association (DISA), on behalf of the Accredited Standards Committee (ASC) X12. All rights reserved. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided “as is” without any express or implied warranty. Note that the copyright on the underlying ASC X12 Standards is held by DISA on behalf of ASC X12. 2011 © Companion Guide copyright by Computer Sciences Corporation.

The information in this document is subject to change. Changes will be posted via the NCTracks website located at https://www.nctracks.nc.gov/content/public/providers/provider-trading-partners.html.

Preface

Companion Guides (CG) may contain two types of data, instructions for electronic communications with the publishing entity (Trading Partner Information) and supplemental information for creating transactions for the publishing entity while ensuring compliance with the associated ASC X12 Implementation Guide (IG) (Transaction Instructions). Either the Trading Partner Information component or the Transaction Instruction component must be included in every Companion Guide. The components may be published as separate documents or as a single document.

The Communications/Connectivity component is included in the Companion Guide when the publishing entity wants to convey the information needed to commence and maintain communication exchange.

The Transaction Instruction component is included in the Companion Guide when the publishing entity wants to clarify the IG instructions for submission of specific electronic transactions. The Transaction Instruction component content is limited by ASC X12's copyrights and Fair Use statement.

Table of Contents

1. Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Overview 1
1.4 References 1
2. Getting Started 2
2.1 Working Together 2
2.2 Trading Partner Registration 2
2.2.1 Trading Partner/Providers Enrollment 2
2.2.2 User Provisioning and Mailbox Creation Steps 3
2.2.2.1 New User Setup Instructions 3
2.2.2.2 User Maintenance Setup Instructions 11
2.2.2.3 User Role Setup Instructions 15
2.2.3 Requirements for Electronic Data Interchange 18
2.2.4 Supported Transactions 18
3. Testing and Certification Requirements 19
3.1 Testing Requirements 19
3.1.1 NCTracks Trading Partner Testing Portal – Enrollment and Access 19
3.1.2 NCTracks Trading Partner Testing Portal – Supported Transactions 19
3.1.3 NCTracks Trading Partner Testing Portal – Outbound Transactions 19
3.1.4 NCTracks Trading Partner Testing Portal – Availability and Support 20
3.2 Certification Requirements 20
3.3 Sample Invite from Trading Partner Certification 21
4. Connectivity / Communications 22
4.1 Transmission Administrative Procedures 22
4.1.1 Retransmission Procedures 22
4.2 Communication Protocols 22
4.2.1 Secure FTP and HTTP 22
4.2.1.1 Transport Encryption 23
4.2.1.2 User ID and Password 24
4.2.1.3 File Naming Standards 24
4.2.1.4 Supported Clients 25
4.2.1.5 Data Exchange Protocols 25
4.2.1.6 FTP Supported Commands 26
4.2.1.7 FTP Integrity Check Commands 27
4.2.1.8 FTP Nontraditional Commands and Unsupported Commands 27
4.2.1.9 Directory View Differences Between Browser Session and FTP Session 28
4.2.2 NCTracks Provider Portal – Batch X12 Submissions 29
4.2.3 CPU-to-CPU Real Time 41
4.2.4 NCTracks Provider Portal – Direct Data Entry 42
4.2.5 CAQH-CORE Phase II Connectivity (270/271 and 276/277) 43

4.2.5.1 SOAP and MIME Attributes for 270/271 and 276/277 44
4.2.5.2 SOAP for 270/271 and 276/277 46
4.2.5.3 MIME for 270/271 and 276/277 49
4.2.6 CAQH-CORE Phase III Connectivity (835 and 820) 57
4.2.6.1 SOAP and MIME Attributes for 835 and 820 58
4.2.6.2 SOAP for 835 and 820 59
4.2.6.3 MIME for 835 and 820 61
4.2.7 CAQH-CORE Phase II and III – Submitting 999 Transactions 64
4.2.7.1 SOAP and MIME Attributes for 999 Submission 64
4.2.7.2 SOAP for 999 Submission 66
4.2.7.3 MIME for 999 Submission 67
4.2.8 SOAP and MIME Error Messages 68
4.2.8.1 SOAP Error Message Examples 69
4.2.8.2 MIME Error Message Examples 72
5. Contact Information 77
5.1 EDI Technical Assistance 77
5.2 Provider/Trading Partner Enrollment 77
5.3 Connectivity and Other Technical Issues 77
5.4 Web Portal Issues 77
5.5 Security and Privacy Issues 77
6. Control Segments / Envelopes 78
6.1 ISA-IEA 78
6.2 GS-GE 78
6.3 ST-SE 79
7. Acknowledgments and Reports 80
7.1 ASC X12 Acknowledgments 80
7.1.1 Negative Interchange Acknowledgment (TA1) Negative File Transfer Status (F-File) 80
7.1.2 Response Specific Information 80
7.1.3 Preadjudication Editing 80
7.1.4 Acknowledgment Examples 81
7.1.4.1 Acknowledgments – Accepted 81
7.1.4.2 Acknowledgments – Rejected 81
7.1.5 Acknowledgments for Batch Transactions 82
7.2 Remittance Advice 83
8. Additional Trading Partner Information 84
8.1 Implementation Checklist 84
8.2 Transmission Examples 84
8.3 Trading Partner Agreement 84
8.4 Frequently Asked Questions 84
8.5 Other Resources 87
8.5.1 NCTracks Fiscal Agent 87
8.5.2 Other Useful Websites 87
Appendix A. Ipswitch Tested FTP Clients 89

A.1 Supported Secure FTP/SSH (and SCP2) Clients 89
A.2 Supported Secure FTP SSL Clients 90
Appendix B. Web Interface 91
B.1 MoveIT Wizard Installation 91
B.1.1 Wizard Requirements 91
B.1.2 Firewall and Proxy Server Issues 91
B.1.3 Internet Explorer 92
B.1.4 Internet Explorer 7.0 or Higher 94
B.1.5 Other Browsers 94
B.1.5.1 Install the Java Wizard 95
B.2 Web Interface – Upload/Download Wizard 95
B.2.1 Upload Wizard 95
B.2.2 Download Wizard 98
Appendix C. 270 SOAP and MIME Samples 101
C.1 270 SOAP Batch Sample 101
C.2 270 SOAP Real-time Sample 102
C.3 270 MIME Batch Sample 103
C.4 270 MIME Real-time Sample 104
Appendix D. 276 SOAP and MIME Samples 105
D.1 276 SOAP Batch Sample 105
D.2 276 SOAP Real-time Sample 106
D.3 276 MIME Batch Sample 107
D.4 276 MIME Real-time Sample 108
Appendix E. 999 Request SOAP and MIME Batch Samples 109
E.1 999 Request SOAP Batch Sample 109
E.2 999 Request MIME Batch Sample 110
Appendix F. 835 SOAP and MIME Batch Samples 111
F.1 835 Request SOAP Batch Sample 111
F.2 835 Request MIME Batch Sample 112
Appendix G. 820 SOAP and MIME Batch Samples 113
G.1 820 Request SOAP Batch Sample 113
G.2 820 Request MIME Batch Sample 114
Appendix H. 999 Submission SOAP and MIME Samples 115
H.1 999 Submission SOAP Batch Sample 115
H.2 999 Submission MIME Batch Sample 116

List of Exhibits

Exhibit 4-1. SFTP Protocol Information 25
Exhibit 4-2. FTPS Protocol Information 25
Exhibit 4-3. FTPES Protocol Information 26
Exhibit 4-4. HTTPS Protocol Information 26
Exhibit 4-5. FTP Commands 27
Exhibit 4-6. FTP Integrity Check Commands 27
Exhibit 4-7. FTP Nontraditional Commands 27
Exhibit B-1. Wizard Status 92
Exhibit B-2. ActiveX Control Block of Wizard Installation 92
Exhibit B-3. Enable ActiveX Wizard Install 93
Exhibit B-4. ActiveX Wizard Install 93
Exhibit B-5. Access Security Settings 94
Exhibit B-6. Access Security Trusted Site Settings 94
Exhibit B-7. Confirmed Trusted Site 94
Exhibit B-8. Java Wizard Install 95
Exhibit B-9. Upload Wizard File Selection 96
Exhibit B-10. Upload Wizard File Options 97
Exhibit B-11. Upload Wizard Progress Bar 97
Exhibit B-12. Download Wizard Options 98
Exhibit B-13. Download Destination Selection 99
Exhibit B-14. Download Wizard Progress Bar 99
Exhibit B-15. Download Wizard Transfer Complete Options 100

1. Introduction

1.1 PURPOSE

This document is intended to provide information from the author of this guide to Trading Partners to give them the information they need to exchange Electronic Data Interchange (EDI) data with the author. This includes information about registration, certification, connectivity, and support, and specific information about control record setup.

1.2 SCOPE

This Trading Partner Information Companion Guide is intended as a resource to assist providers, clearinghouses, service bureaus, and all other trading partners of the North Carolina Division of Health Benefits (DHB), Division of Mental Health (DMH), Division of Public Health (DPH), and Office of Rural Health and Community Care (ORHCC) in successfully conducting EDI of administrative health care transactions using NCTracks, the multi-payer system supporting these payers. This document provides instructions for enrolling as an NCTracks Trading Partner, obtaining technical assistance, initiating and maintaining connectivity, sending and receiving files, testing, and other related information. This document does not provide detailed data specifications, which are published separately by the industry committees responsible for their creation and maintenance.

1.3 OVERVIEW

This guide provides communications-related information that a Trading Partner needs to enroll as a Trading Partner, obtain support, format the ISA and GS envelopes, submit tests, and exchange production transactions with NCTracks.

Providers who are not enrolled in NCTracks cannot enroll as Trading Partners until registered and credentialed with NCTracks. Please contact NCTracks Enrollment at 1-800-688-6696 or visit the following website:

https://www.nctracks.nc.gov/content/public/providers/provider-enrollment.html

1.4 REFERENCES

The NCTracks website contains links to all forms and related information for enrollment as a Trading Partner. Refer to http://www.nctracks.nc.gov/index.html for additional information and a variety of useful quick links such as FAQs, enrollment instructions, and complete set of companion guides on NCTracks.

For NCTracks Health Insurance Portability and Accountability Act (HIPAA) Companion Guides, please visit the following website. Transaction companion guides are also available within the Trading Partner Testing Portal, which is a self-service EDI test site for NCTracks trading partners.

http://www.nctracks.nc.gov/provider/guides/index.html

For NCTracks trading partner enrollment information, please visit the following website:

https://www.nctracks.nc.gov/provider/providerEnrollment/

2. Getting Started

2.1 WORKING TOGETHER

NCTracks Support Services Contact Information
Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

Website: http://www.nctracks.nc.gov/provider/index.html

EDI Technical Assistance
Phone: 1-800-688-6696, option #1

Email: NCMMIS_EDI_SUPPORT@gdit.com

Website: http://www.nctracks.nc.gov/provider/index.html

Companion Guides: http://www.nctracks.nc.gov/provider/guides/index.html

Provider/Trading Partner Enrollment
Currently Enrolled Provider (CEP), Billing Agent Enrollment:

Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

Website: https://www.nctracks.nc.gov/provider/providerEnrollment/

NCTracks Enrollment:

Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

https://www.nctracks.nc.gov/content/public/providers/provider-enrollment.html

2.2 TRADING PARTNER REGISTRATION

2.2.1 Trading Partner/Providers Enrollment

An EDI Trading Partner is any entity (provider, billing service, software vendor, employer group, financial institution, clearinghouse, etc.) that transmits electronic data to or receives electronic data from another entity.

Trading Partner registration, which includes electronic signature of the Trading Partner Agreement (TPA) and generation of the Transaction Supplier Number (TSN), is an online process, and the instructions are provided in this document. Clearinghouses, service bureaus, trading partners, billing agents, and other entities that intend to exchange electronic transactions with NCTracks must sign the TPA and be enrolled into NCTracks.

Successful enrollment is required before proceeding with exchange of EDI data.
Currently Enrolled Provider (CEP), Billing Agent Enrollment:

Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

Website: https://www.nctracks.nc.gov/provider/providerEnrollment/

NCTracks Enrollment:

Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

https://www.nctracks.nc.gov/content/public/providers/provider-enrollment.html

Please note that all entities should obtain NCID (North Carolina Identity Management) credentials before enrolling into NCTracks. For information on obtaining NCID credentials, please refer to the following websites:

NCID Registration: https://ncid.nc.gov

NCID FAQs: https://www.ncid.its.state.nc.us/NCID_FAQ2.asp

2.2.2 User Provisioning and Mailbox Creation Steps

Any users registered and provisioned in the Billing Agent application on or before June 24, 2013 will automatically be provisioned into NCTracks and their mailboxes will be created before Go-Live.

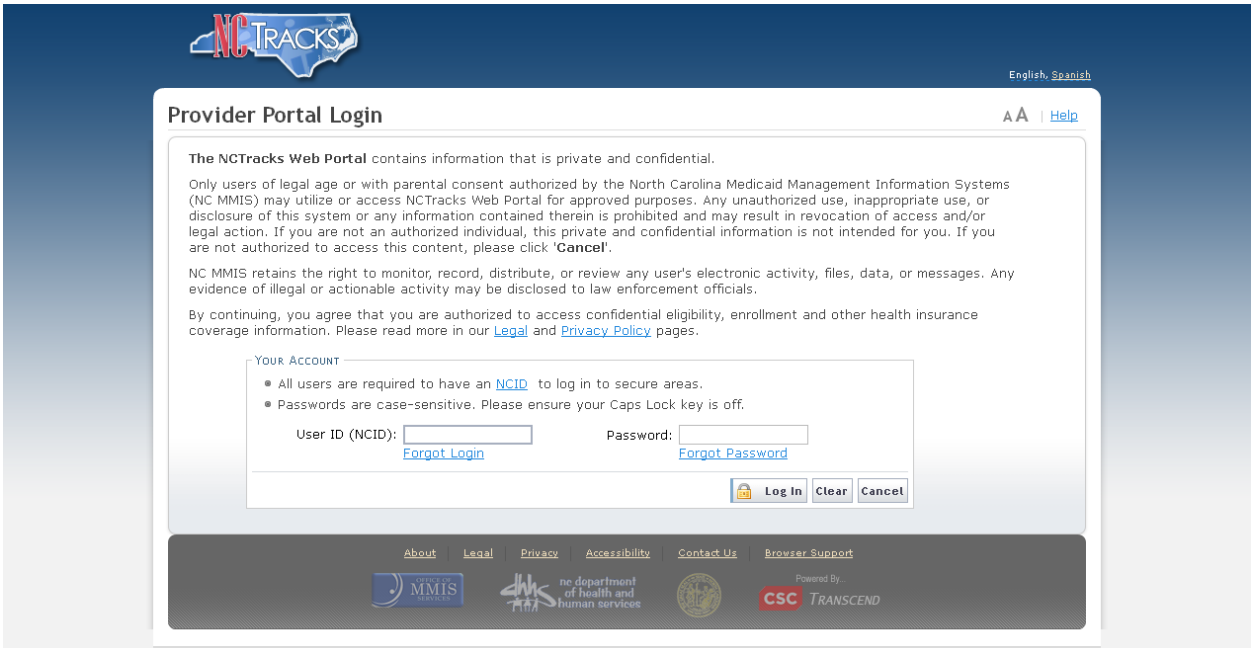
Trading Partners can provision themselves to submit their files via MoveIT/FTP-Batch and Council for Affordable Quality Healthcare Committee on Operating Rules for Information Exchange (CAQH CORE) methodologies. Following are the steps for those Trading Partners (clearinghouses, billing agents, etc.) who will be provisioning themselves after July 1, 2013. These steps are usually performed by the office administrator or user administrator. Users whose NCIDs are provisioned to submit or receive X12 transactions will have their own individual mailboxes.

2.2.2.1 New User Setup Instructions

This series of web pages allows the office administrator or user administrator to create a new user in the NCTracks application.

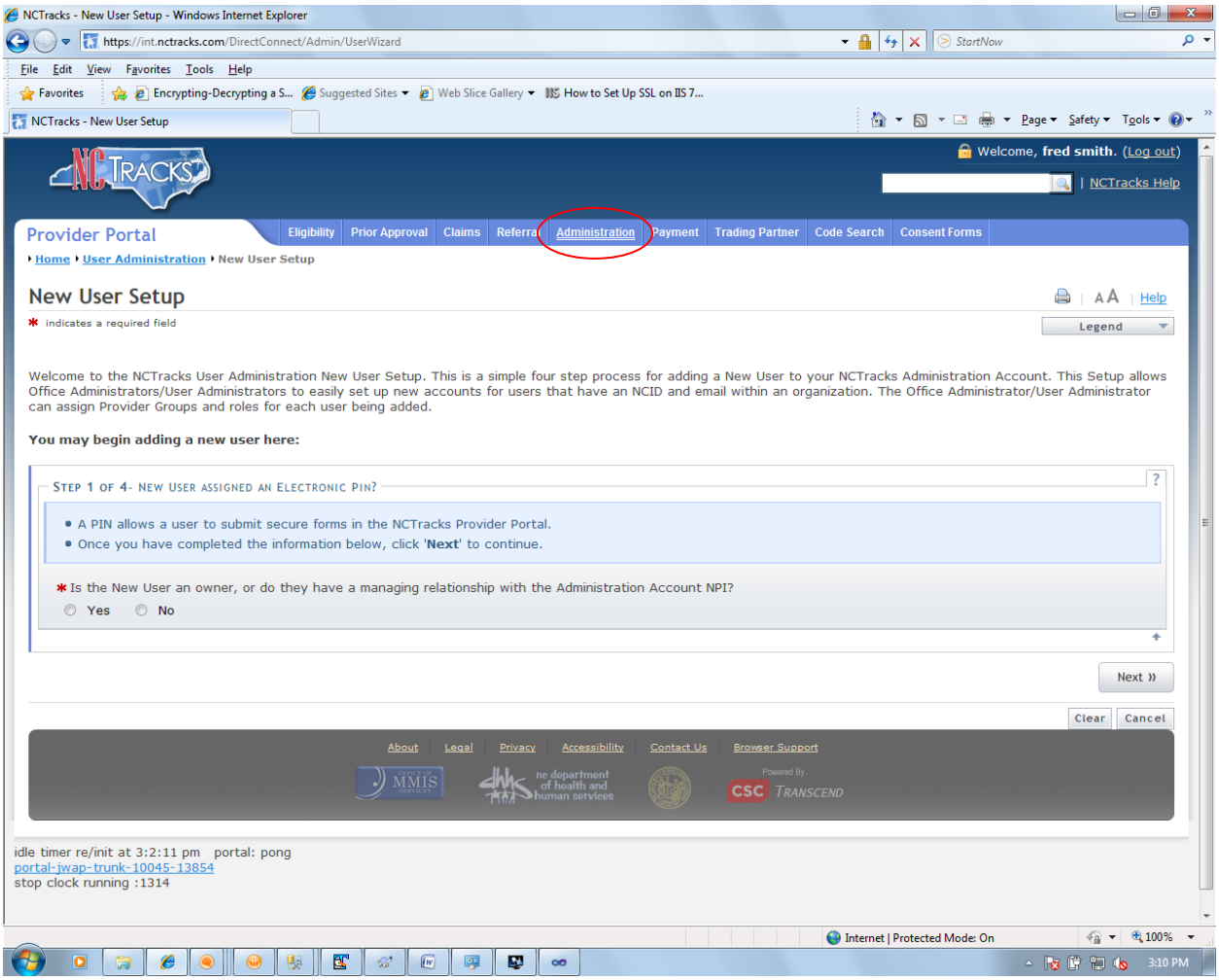
Step 1:
Log in to https://www.nctracks.nc.gov.

Enter your NCID and Password and click the **Log In** button.

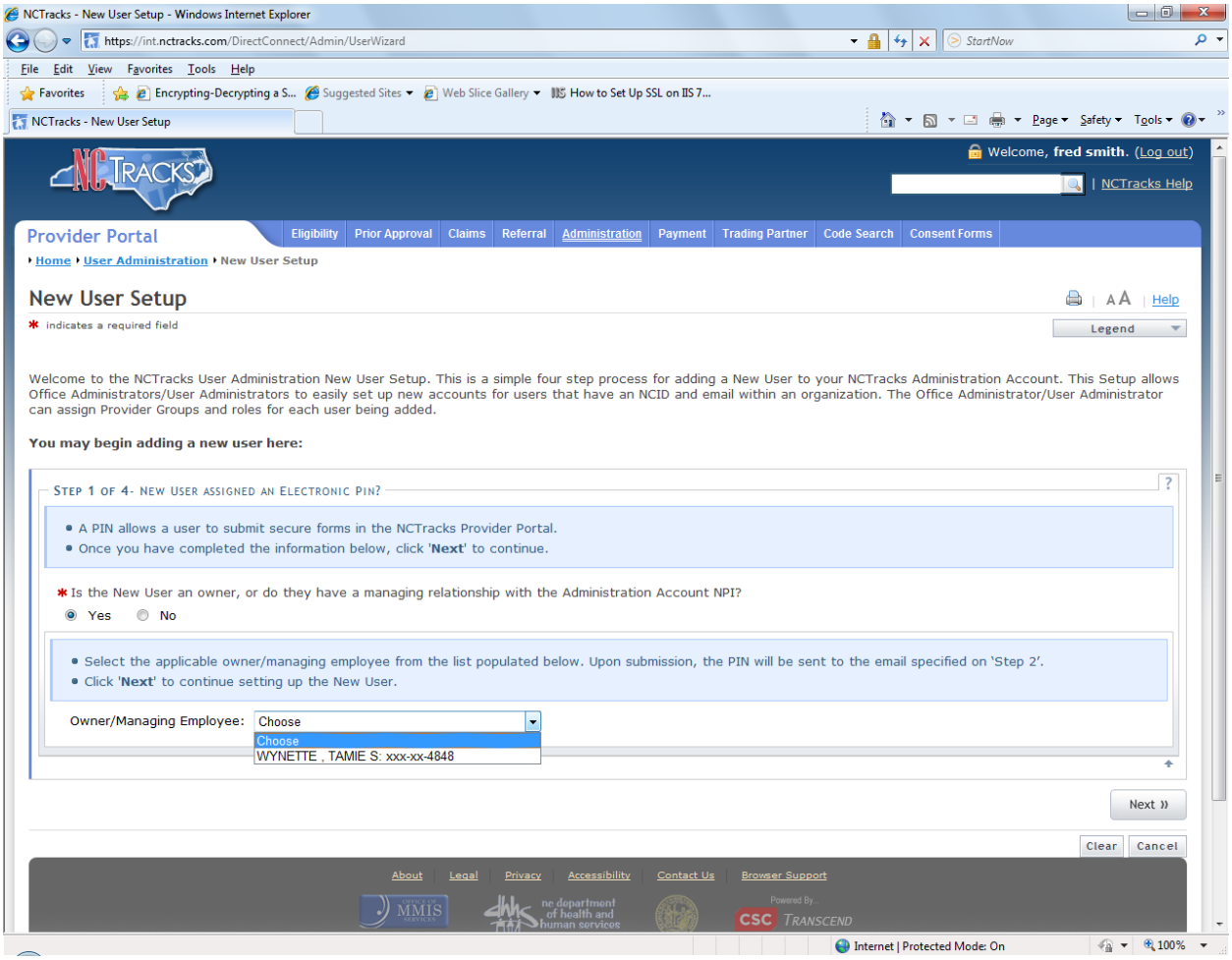


portal-jwap-trunk-10060-14974

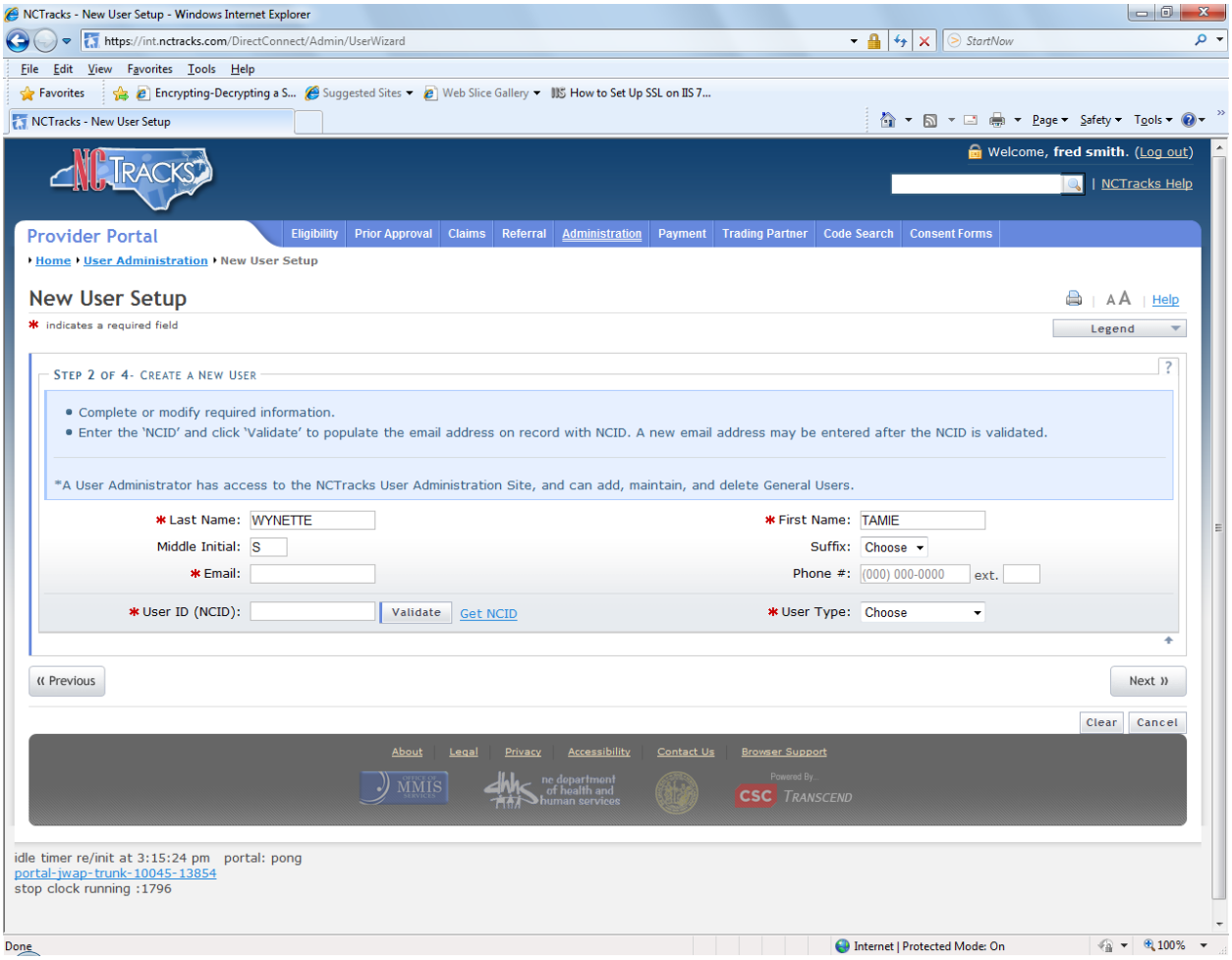
Step 2:
The page in this step determines whether the user you are creating is an owner/managed relationship user. Select **No** and click the **Next** button if you are not creating an owner/managed relationship user.



If you are creating an owner/managed relationship user, select **Yes** and select the Owner/Managing Employee from the drop-down field. Click the **Next** button.

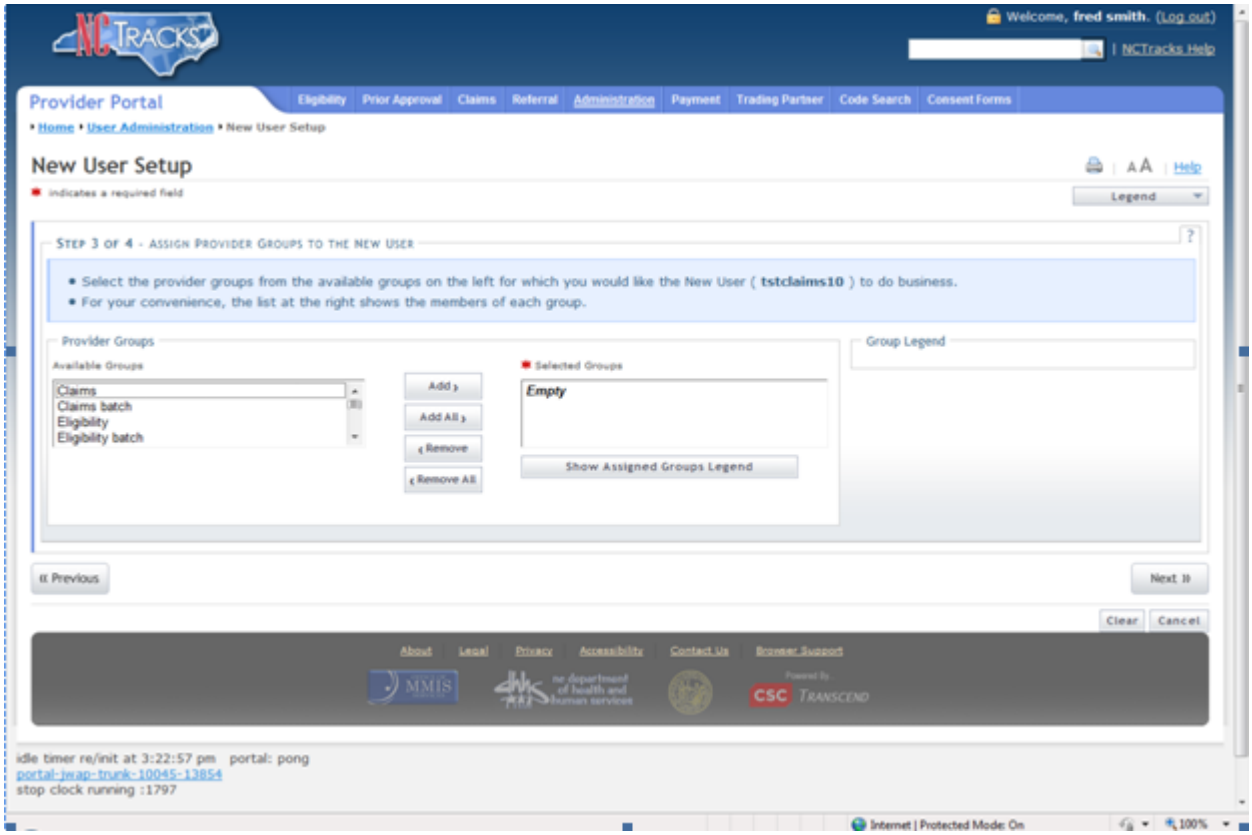


Step 3:
At a minimum, enter all the required data elements for the page. When entering the User ID (which is an NCID), click the **Validate** button to ensure the NCID is valid. The system will populate the **Email** field with the email address that was used when the NCID was created. Click the **Next** button.



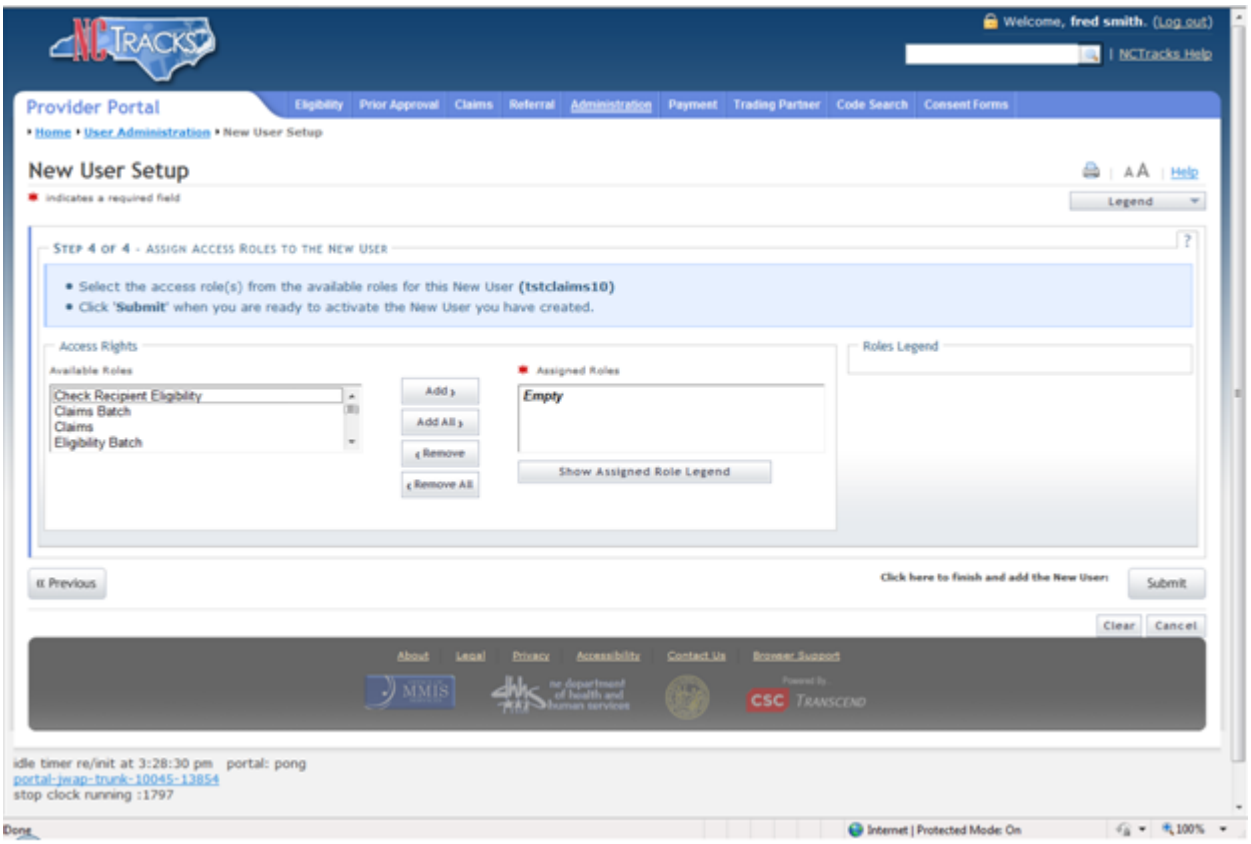
Step 4:
Select a Provider Group from the Available Groups list on the left side of the page, and click the **Add** button to add the group to the Selected Groups list on the right side. The Selected Groups list contains the selected Provider Groups for the user you are creating. A Provider Group contains the National Provider Identifiers (NPIs) for which the user can bill. To view the NPIs in a Provider Group, select the group from the Selected Groups list and click the **Show Assigned Groups Legend** button. A list of all the NPIs in the selected group will display in the **Group Legend** field.

After selecting all the Provider Groups for the user, click the **Next** button.

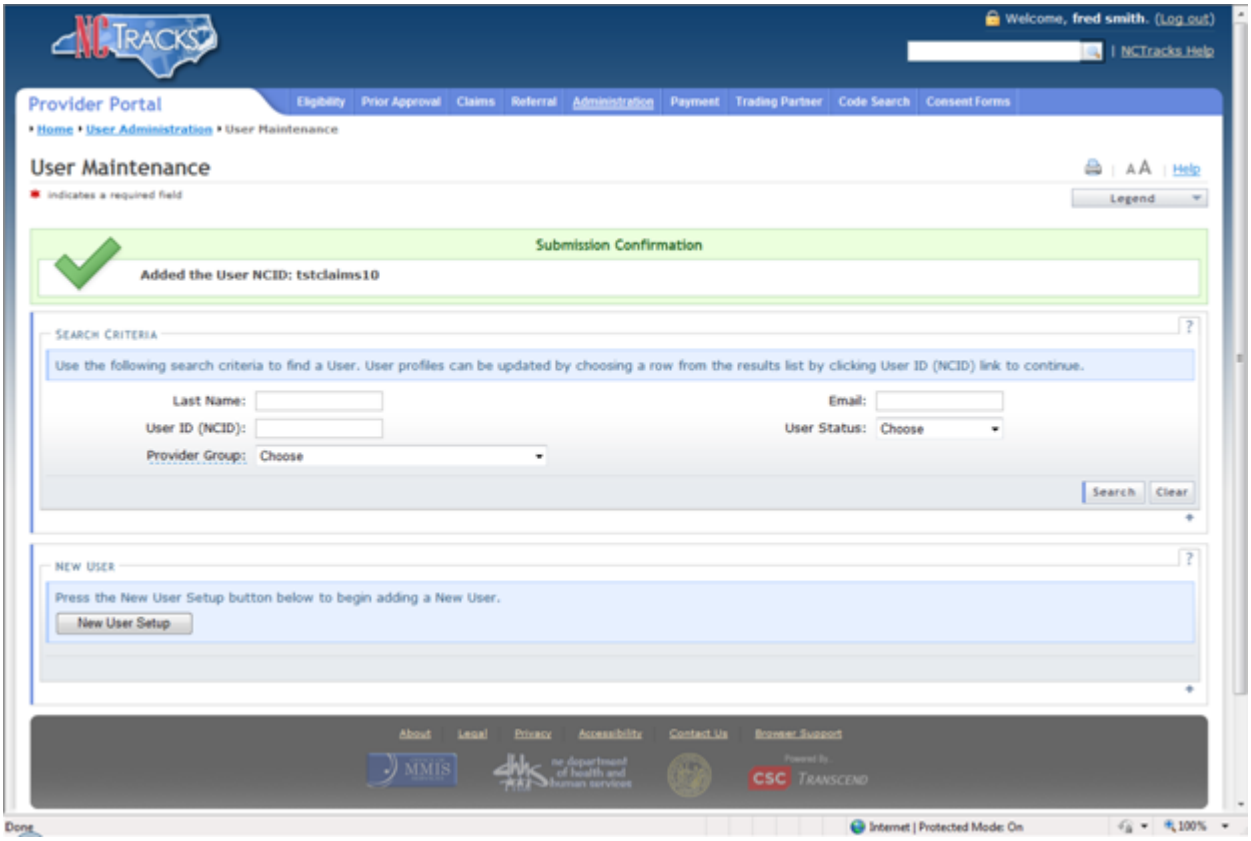


Step 5:
Select a role from the Available Roles list on the left side of the page, and click the **Add** button to add the role to the Assigned Roles list on the right side. The Assigned Roles list contains the roles that the user can perform in the Provider portal, for the user you are creating. To view an explanation of each role, select a role from the Assigned Roles list and click the **Show Assigned Role Legend** button. A list of all the roles will display in the **Roles Legend** field.

After selecting all the roles for the user, click the **Submit** button.



This page displays the results of the New User Setup. The User NCID was added as a user.

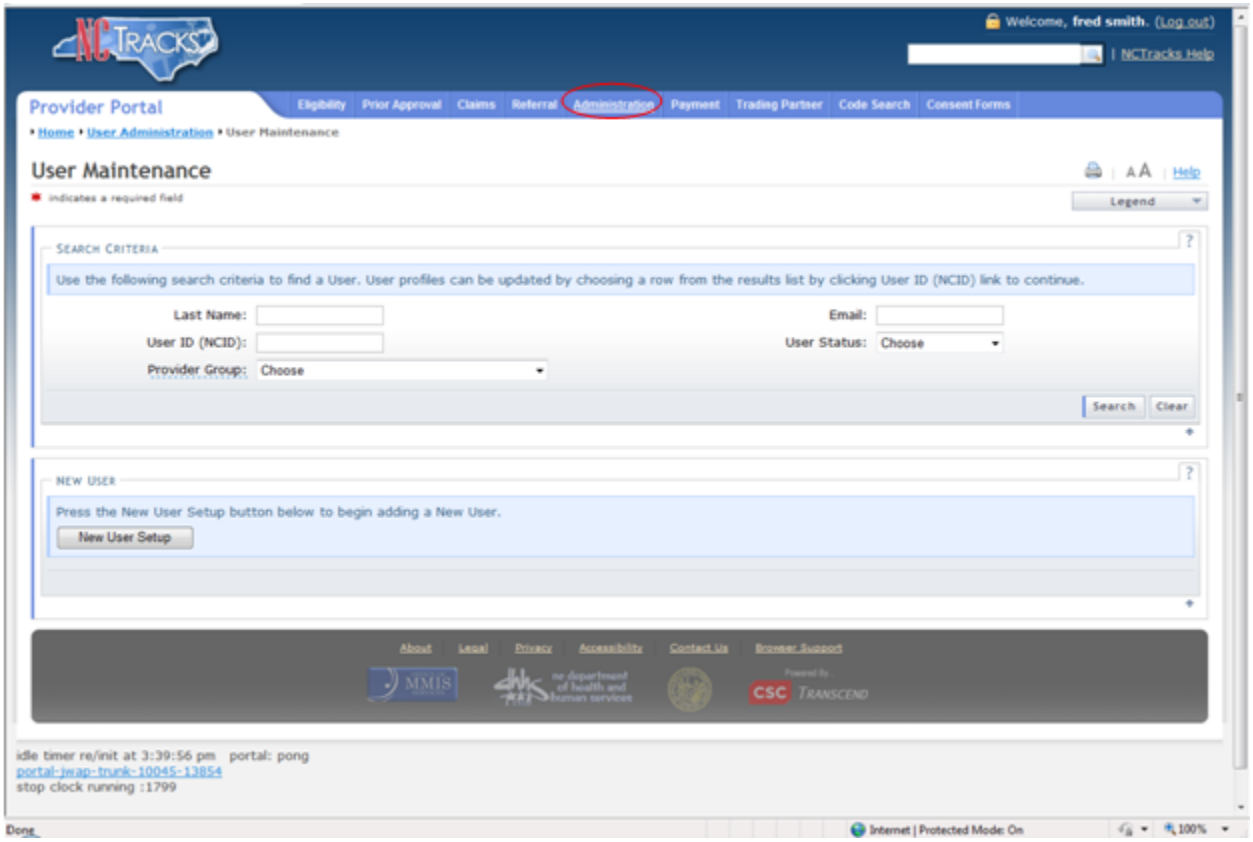


2.2.2.2 User Maintenance Setup Instructions

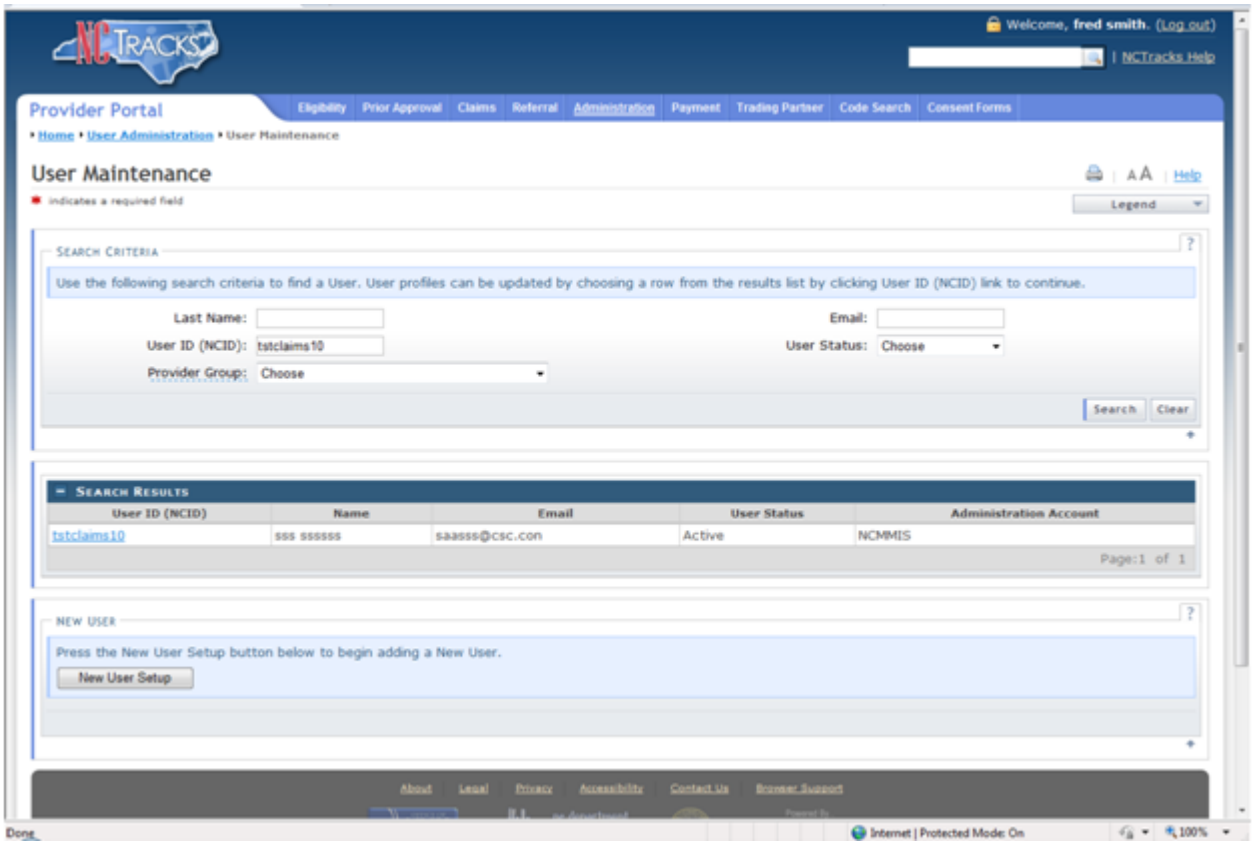
This series of web pages allows the office administrator or user administrator to change a user's demographic information, Provider Groups, and roles for the Provider portal.

Step 1:

This page allows you to search for a user to change their data or go the New User Setup pages.



You can search for a user by entering one or more of the Search Criteria data elements and clicking the **Search** button. If you leave the Search Criteria blank and click the **Search** button, all users will display.



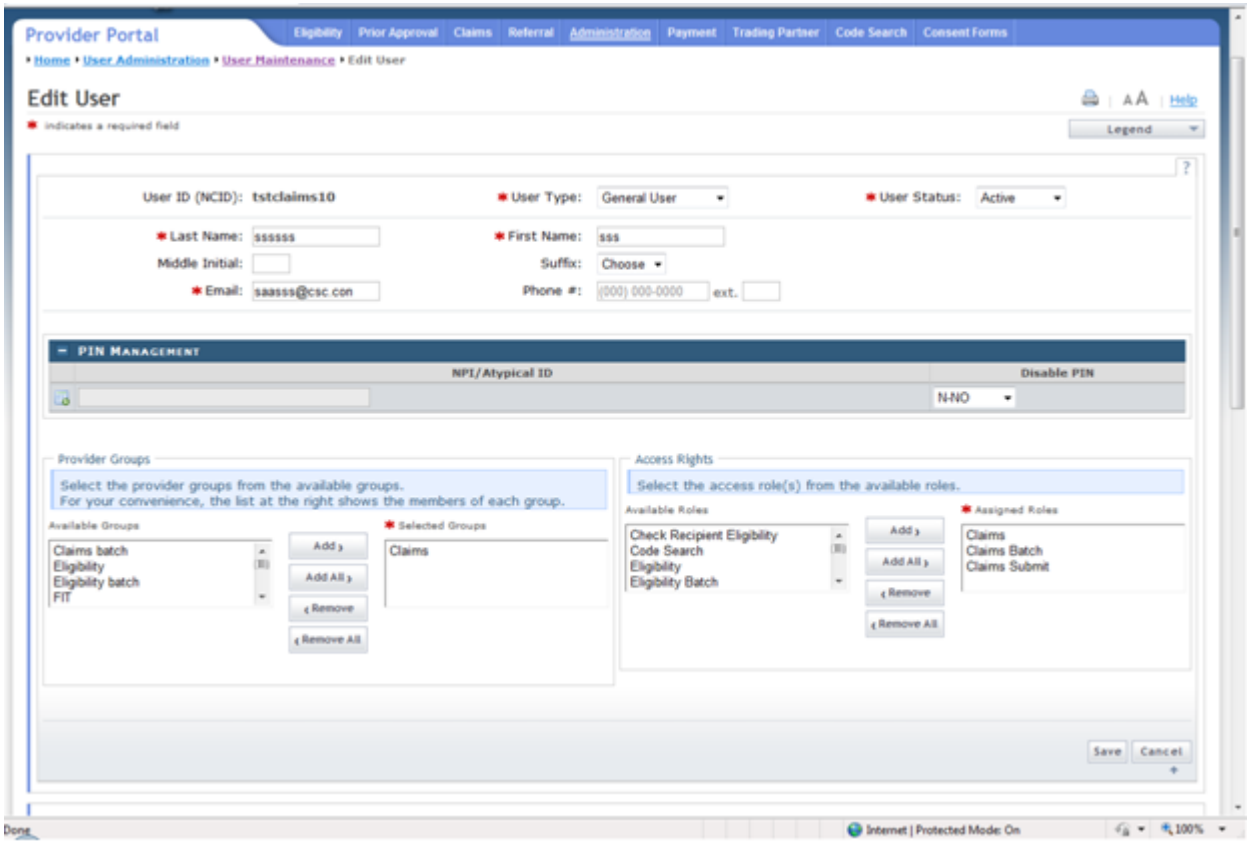
Step 2:
After searching for a user, select the User ID (NCID) found in the Search Results grid to go to the Edit User page.

On the Edit User page, you can change the user's demographic information found at the top of the page. You can also change the Provider Groups and roles assigned to the user.

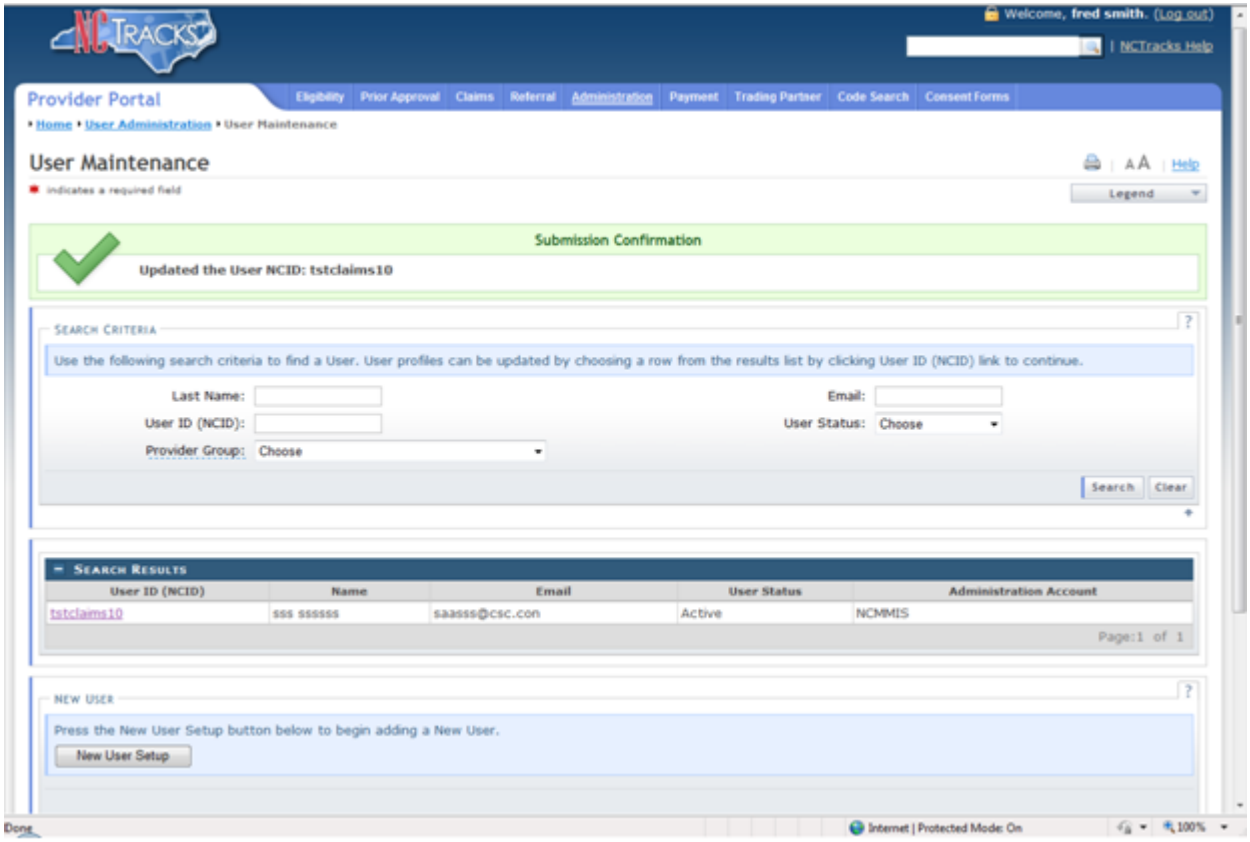
The PIN Management grid allows you to determine if the NPI assigned to the user is PIN worthy, meaning you can disable or enable the NPI for PIN checking when submitting a Provider Application. The PIN Management grid displays the NPIs/Atypical IDs assigned to the user. If you enable the PIN for this NPI/Atypical ID, then during the submission of a Provider Application a request will be made to the user to enter their PIN. If you disable the PIN, then no request for a PIN will be made during the submission of the Provider Application.

A Provider Application can be found in the Provider portal and is based on an NPI/Atypical ID.

After you have made your changes to the user's information, click the **Save** button.



Step 3:
This page displays the results of the Edit User. The user was updated.

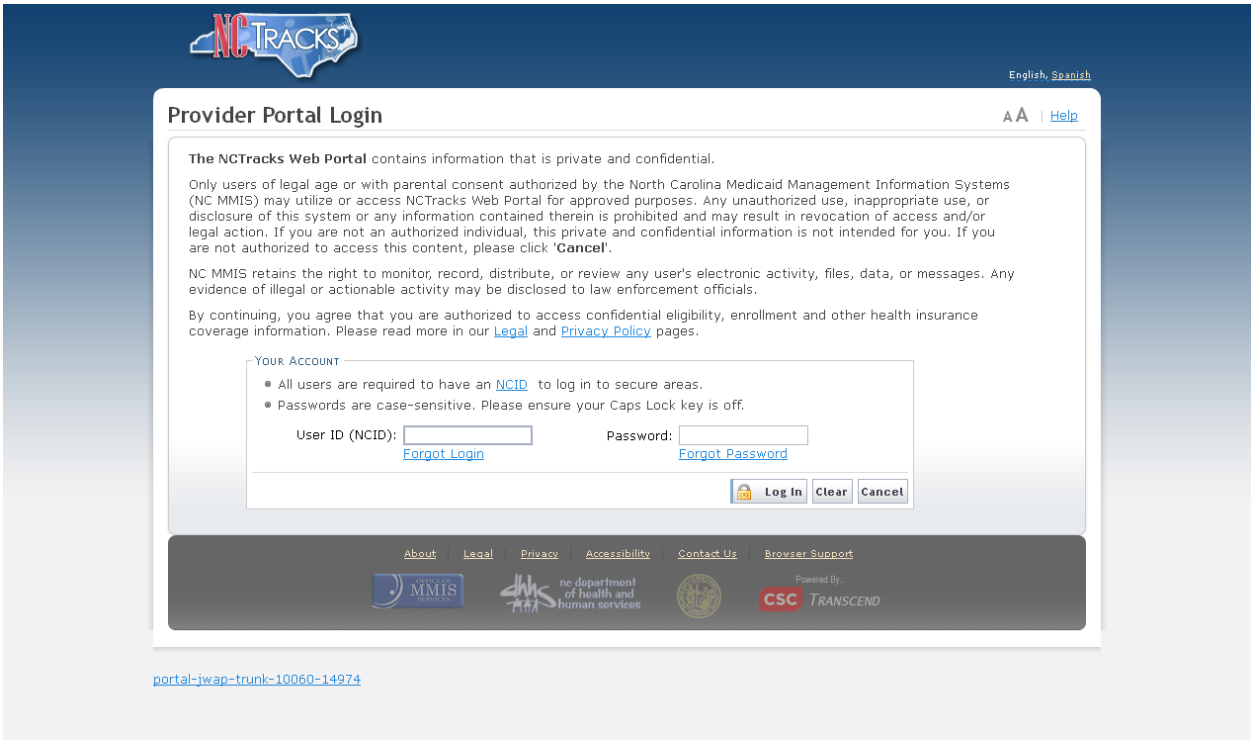


2.2.2.3 User Role Setup Instructions

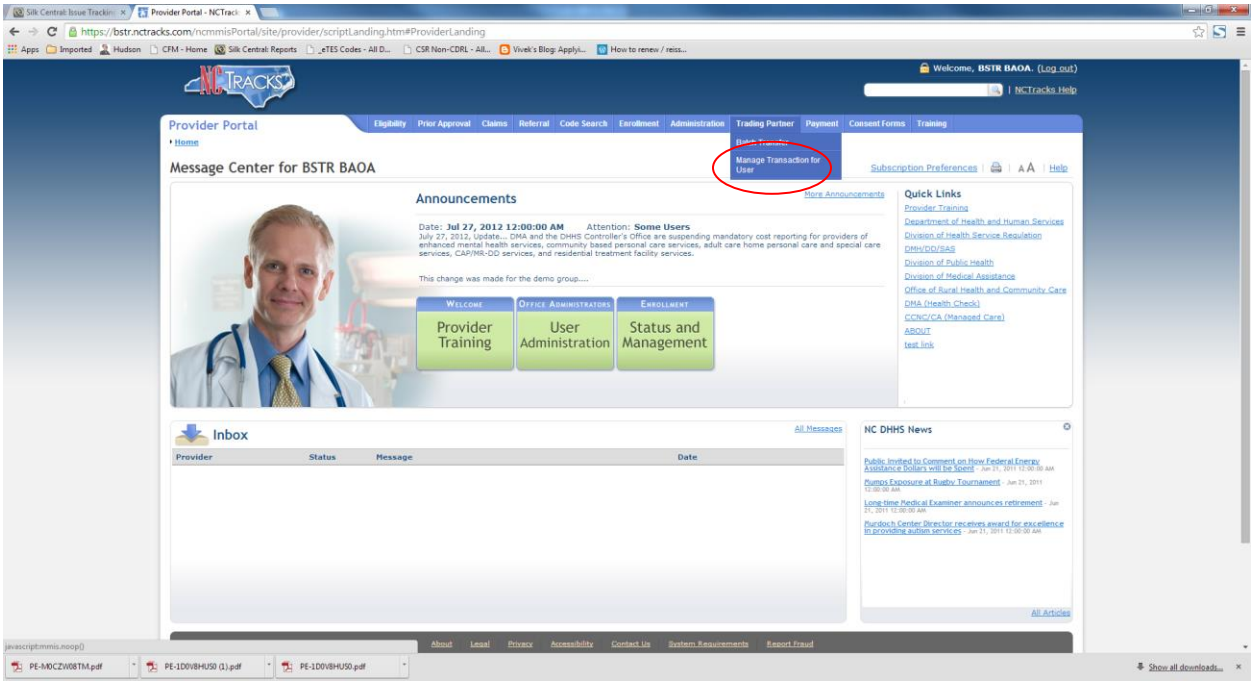
This series of web pages allows the office administrator or user administrator to create roles for existing users in the NCTracks application.

Step 1:
Log in to https://www.nctracks.nc.gov.

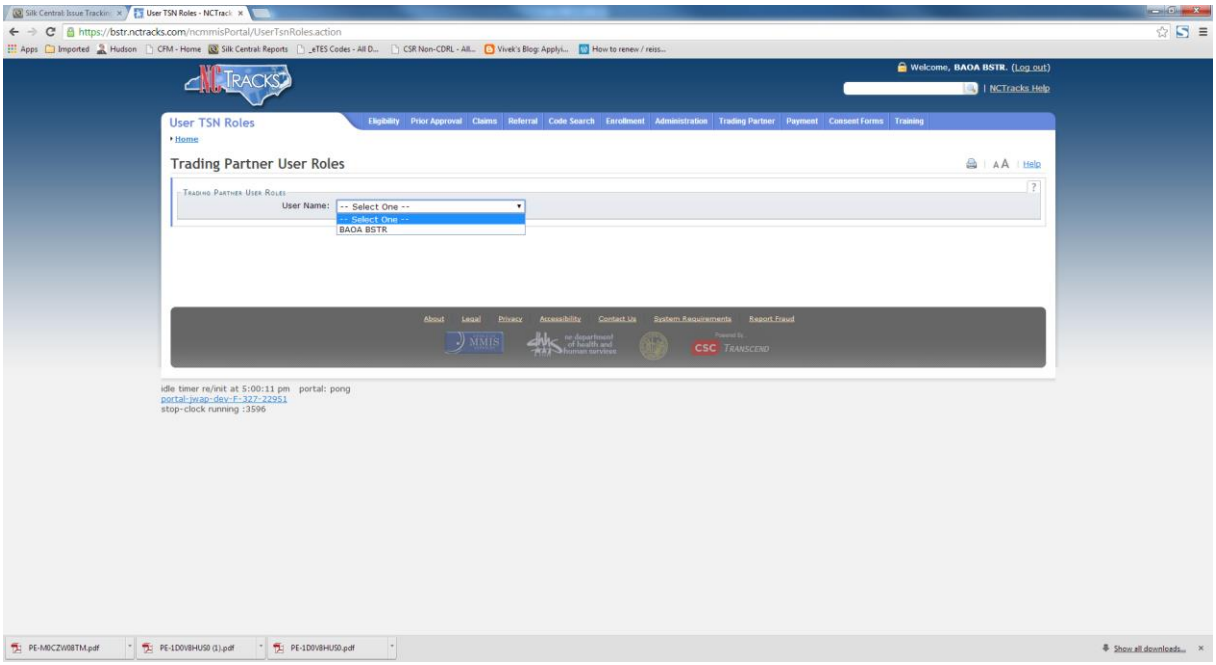
Enter your NCID and Password and click the **Log In** button.



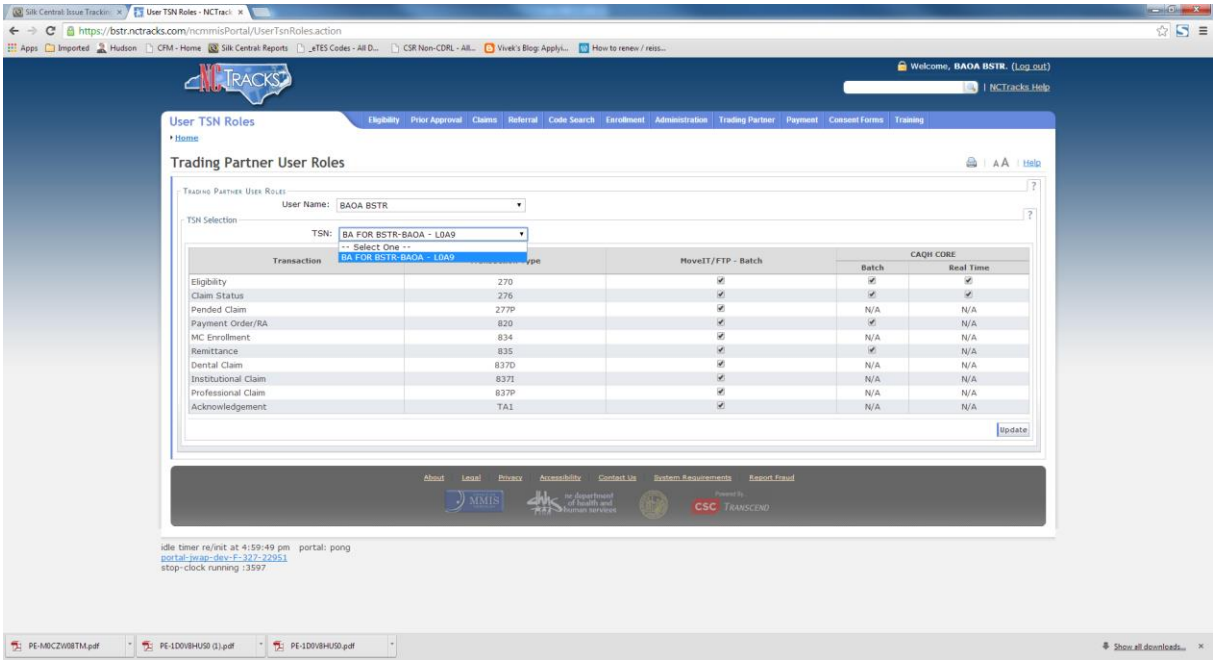
Step 2:
Select the **Trading Partner** menu and select the **Manage Transaction for User** menu option.



Step 3:
The **User Name** drop-down field displays a list of all users, by first name and last name, working under the office administrator or user administrator. Select the User Name whose user role will need to be updated.



Step 4:
The Trading Partner User Roles screen displays a list of Transactions and the Transaction Types assigned to the Trading Partner. The office administrator or user administrator can select user roles based on MoveIT/FTP-Batch and CAQH CORE methodologies. Click the **Update** button in the bottom right corner to save the selections.



2.2.3 Requirements for Electronic Data Interchange

An EDI Trading Partner is any entity (provider, billing service, software vendor, employer group, financial institution, clearinghouse, etc.) that transmits electronic data to or receives electronic data from another entity. For information about available NCTracks Access Methods, refer to Section 4.2, Communication Protocols.

Prior to establishing electronic access with NCTracks, any entity that plans to exchange electronic data with NCTracks must obtain a TSN through the enrollment process described in Section 2.2.1, Trading Partner/Providers Enrollment. A TSN is used to identify a submitter. A TSN may also be used in conjunction with an NPI/API to set up electronic routing of Remittance Advices. In addition to obtaining a TSN, all Trading Partners are also required to go through the certification process outlined in Section 3, Testing and Certification Requirements.

2.2.4 Supported Transactions

NCTracks supports several HIPAA-compliant electronic health care transactions. The following table lists the inbound and outbound 5010 transactions supported by NCTracks. NCTracks does not support any of the 4010 transactions or the National Council for Prescription Drug Programs (NCPDP) 5.1 transactions. NCTracks supports processing of both Fee For Service and Encounter claims.

	Direct Response(s)		Routed Response(s)
Request	**Batch**	**Real-time**	**Batch Only**
270	F-FILE, TA1, 999, 271	GS99, TA1, 999, 271	N/A
276	F-FILE, TA1, 999, 277	GS99, TA1, 999, 277	N/A
834I	F-FILE, TA1, 999	N/A	N/A
			834O
			820
837I	F-FILE, TA1, 999	GS99, TA1,999, U277	835, 277P (only for Pended claims)
837P	F-FILE, TA1, 999	GS99, TA1,999, U277	835, 277P (only for Pended claims)
837D	F-FILE, TA1, 999	GS99, TA1,999, U277	835, 277P (only for Pended claims)
NCPDP (B1, B2, B3, E1, N1, N2, N3)	N/A	GS99; NCPDP D.0	NCPDP D.0 responses, 835

3. Testing and Certification Requirements

3.1 TESTING REQUIREMENTS

The NCTracks Trading Partner Testing Portal enables Trading Partners to conduct self-service testing of inbound EDI transactions. Sample outbound transaction files are also available for testing.

3.1.1 NCTracks Trading Partner Testing Portal – Enrollment and Access

The NCTracks Trading Partner Testing Portal (through the Ramp Management Tool) is provided to enable NCTracks trading partners to independently test inbound batch EDI transactions in a self-service environment. The Trading Partner Agreement (TPA) must be signed in the Trading Partner Testing Portal before submitting the test transactions.

Test transactions submitted to the NCTracks Trading Partner Testing Portal undergo compliance level validation and certain specific NCTracks validations relative to X12 compliance. The Trading Partner Testing Portal is designed to lead a trading partner through the required steps to receive certification to submit EDI transactions. These steps are defined in a program for each transaction the trading partner intends to submit.

3.1.2 NCTracks Trading Partner Testing Portal – Supported Transactions

The NCTracks Trading Partner Testing Portal supports testing and certification of the following 5010 X12 inbound transactions:

- 270 – Eligibility Inquiry
- 276 – Claims Status Request
- 834I – Benefit Enrollment and Maintenance
- 837I – 837 Institutional claim
- 837P – 837 Professional claim
- 837D – 837 Dental claim

Note: Switch vendors who submit NCPDP transactions will not go through the certification process. Additionally, after being certified, Trading Partners will not be submitting these transactions into any NCTracks test regions.

3.1.3 NCTracks Trading Partner Testing Portal – Outbound Transactions

Outbound transactions are not supported through the NCTracks Trading Partner Testing Portal. This includes the 271, 277, 820, 834 outbound, and 835 transactions.

However, NCTracks will provide a sample X12 file for trading partners to download and perform testing of their software using NCTracks-generated outbound transactions. The sample file will contain generic data and will not be customized for a given trading partner or provider. There will not be any further validation or certification process on any of the outbound transactions.

3.1.4 NCTracks Trading Partner Testing Portal – Availability and Support

The NCTracks Trading Partner Testing Portal is a self-service portal, so it is generally available for testing at all times.

Support will be available during normal business hours, from 9:00 a.m. to 5:00 p.m. EST, by calling the NCTracks EDI Support Team at 1-800-688-6696, option #1 or emailing at NCMMIS_EDI_SUPPORT@gdit.com.

3.2 CERTIFICATION REQUIREMENTS

NCTracks certifies transaction compliance and requires certification from any external entity to submit inbound X12 transactions. The NCTracks Trading Partner Testing Portal is designed to lead a trading partner through the required steps to receive certification to submit EDI transactions. These steps are defined in a program for each transaction the trading partner intends to submit.

- Trading Partners will receive an invite with a logon ID and password via email from the Trading Partner Testing Portal.
- Trading Partners will download the TPA, sign, and upload the TPA to the Trading Partner Testing Portal.
- Trading Partners will sign up for the programs (transactions) for which they need certification.
- Trading Partners will submit test transactions into the Trading Partner Testing Portal to be validated for compliance checking and NCTracks rules.
- Trading Partners can log issues using the Ramp Management (RM) tool or can call or email the CSRA EDI Support helpdesk.
- After Trading Partners are certified in RM, they will have the opportunity to submit the surveys associated with the program.
- For Trading Partners who had received the original invite to participate in the certification process but did not enroll or complete the process, periodic reminder emails will be sent by the NCTracks EDI team.

The NCTracks Trading Partner Testing Portal provides the trading partner with the instructions for completing all of these steps and tracks the trading partner’s progress within the programs they are performing. The self-service testing tool also provides instructions for logging any issues using the Trading Partner Testing Portal, as well as instructions for calling or emailing the CSRA EDI Support helpdesk.

3.3 SAMPLE INVITE FROM TRADING PARTNER CERTIFICATION

Subject: Welcome to the NCTracks Trading Partner Testing Community

Dear Trading Partner,

Test Trading Partner has been invited to the NCTracks Trading Partner Testing Community.

The Community provides a web-based validation tool for you to test transaction compliance with the specifications of NCTracks Testing Portal.

We welcome you to take advantage of this service today. Below you will find a link to the web site and your username and password to log on and begin testing.

URL: https://sites.edifecs.com/?nctracks

User Name: based upon last name, first name

Password: (initial password is system generated)

If you have any questions, please feel free to contact us at NCMMIS_EDIT_SUPPORT@gdit.com or 1-800-688-6696. We look forward to hearing from you.

Sincerely,

NCTracks Testing Portal
1-800-688-6696

4. Connectivity / Communications

4.1 TRANSMISSION ADMINISTRATIVE PROCEDURES

Production transmissions must use the appropriate indicator to be directed to the correct environment. For details about available NCTracks Access Methods, refer to Section 4.2, Communication Protocols.

4.1.1 Retransmission Procedures

In the event of an interrupted communications session, the Trading Partner only needs to reconnect and initiate their file transfer as they normally do.

If a file fails the preadjudication process, errors must be corrected before retransmission. It is recommended that transmitted files that were rejected be assigned new Interchange, Group, and Transaction Control Numbers.

4.2 COMMUNICATION PROTOCOLS

The following communication methods are available for the exchange of electronic transactions with NCTracks, also known as NCTracks Access Methods:

- Secure FTP Batch Submissions
- NCTracks Provider Portal Batch Submissions
- CPU-to-CPU Real-time Submissions
- NCTracks Provider Portal Direct Data Entry
- CAQH-CORE Phase II and Phase III

4.2.1 Secure FTP and HTTP

This section provides guidance and information to NCTracks business partners that need to establish a data exchange process with the NCTracks claims processing system of the North Carolina Department of Health and Human Services (NC DHHS). NCTracks has deployed a Managed File Transfer (MFT) system based on the Ipswitch, Inc. MoveIT Family of secure file processing, storage, and transfer products. The MFT system provides secure business-to-business file transfers with secure Internet-based file transfer capabilities.

Exchanging information with NCTracks can be accomplished using different tools and procedures and is dependent on the business partner’s current capabilities. Physical connectivity is accomplished via the Internet.

There are three data exchange protocols available to business partners:

1. Secure File Transfer Protocol (SFTP)
2. File Transfer Protocol Secure Implicit (FTPS)
3. File Transfer Protocol Secure Explicit (FTPES)

Providers, clearinghouses, service bureaus, and all other trading partners of the North Carolina DHB, DMH, DPH, and ORHCC also have the ability to exchange data with NCTracks via the Hypertext Transfer Protocol Secure (HTTPS) protocol.

A secure File Transfer Protocol (FTP) is the standard process for batch authorization transmissions. Secure FTP allows users to transfer files from their computers directly to NCTracks. HTTPS and secure FTP sessions are done strictly via an internet connection.

NCTracks supports the secure exchange of data with external organizations using HTTPS and secure FTP. The NCTracks FTP servers support the SSH File Transfer Protocol (SFTP-3) and SSL-based FTP (Implicit and Explicit) with compression (zlib) for the secure transfer of production data files. The client software that transmits data from NCTracks to external systems uses the SSL or SH-2 and SFTP-3.

4.2.1.1 Transport Encryption

During transport, the NCTracks MFT system uses SSL or SSH to encrypt communications. The strength of the encryption used during SSL-based web transport FTPS is 128-bit or 256-bit. SFTP supports both 128- and 256-bit encryption.

4.2.1.1.1 Encryption Algorithms

The NCTracks MFT system supports the following encryption algorithms:

- AES256-cbc
- AES128-cbc
- twofish256-cbc
- twofish128-cbc
- twofish-cbc
- blowfish-cbc
- 3DES-cbc (also known as “triple-DES”)

4.2.1.1.2 Hash Algorithms

The NCTracks MFT system supports the following (keyed) hash algorithms:

- HMAC-MD5
- HMAC-SHA1
- HMAC-MD5-96
- HMAC-SHA1-96

4.2.1.1.3 Compression Algorithms

The NCTracks MFT system supports the following compression algorithms:

- none
- zlib (also known as “gzip”)

4.2.1.1.4 Storage Encryption

The NCTracks MFT system stores all files on disk using Federal Information Processing Standard (FIPS) 140-2 validated 256-bit Advanced Encryption Standard (AES). The NCTracks MFT system also overwrites just-deleted files with random bytes to prevent encrypted files from lingering on a physical disk after users have deleted them.

4.2.1.1.5 Integrity Checking

When certain file transfer clients are used with the NCTracks MFT system, the integrity of transferred files will be confirmed. All NCTracks MFT system secure FTP and web-based clients (including the upload/download Wizard) support integrity checking.

4.2.1.2 User ID and Password

Trading Partners will use their respective NCID and Password to log in to the FTP website. The NCID must be provisioned in NCTracks before files are sent through the FTP website.

If a user attempts to sign on to a valid account with an incorrect password more than three times, their account will be locked out and administrators will be notified via email. Account lockout lasts 60 minutes.

4.2.1.3 File Naming Standards

Trading Partners must follow the file naming standards listed in this section when submitting inbound X12 transaction files into the “IN” folder of their mailboxes. If the files do not follow these standards, they will be rejected and placed on the “Reject” folder within their respective mailboxes. There are no specific file naming standards for inbound transactions other than the exceptions noted below.

Naming Standards for Inbound Transactions

File Extensions not Accepted

*.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd, *.pif, *.pot, *.reg, *.scr, *.sct, *.shb, *.shs, *.sys, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh

Disallowed Special Characters on File Names

Hyphen (-), asterisk (*), question mark (?)

Duplicate File Names

Files with the same naming convention (duplicate file names) are not allowed within the 30-day period from initial submission. The files submitted by users will be stored on MoveIT for the 30-day period. After 30 days, the files will be purged and archived. Users can submit the duplicate file names after the files are purged from MoveIT.

Zip Files

Submitters can also send in zipped files; however, only one file per zip file is allowed. If more than one file is part of the zip file, the zip file will be rejected.

Deletion of Submitted Files

After an input file submission is done, the submitter will not be able to delete the input file from MoveIT.

Naming Standards for Outbound Transactions

The following is the naming convention standard for outbound transactions:

[R/F]-[Mailbox ID]-[Timestamp]-[File ID]-[Provider Number]-[Transaction Type]-ISA-0001-.X12

Example:
R-BXA12345-140628112722-1417900000000022FF-1234567890-5T-ISA-00001-.x12

Node Name	# of Characters	Description
R/F	1	R: Response F: File
Mailbox ID	8	Alphanumeric characters
Timestamp	12	Timestamp format: YYMMDDHHMMSS
File ID	18	Alphanumeric characters; last 2 characters are always FF
Provider Number	Up to 10	NPI or Atypical ID
Transaction Type	2	01 = TA1 02 = F-File 03 = 999 5A = 820 5E = 834 5R = 277P 5T = 835 09 = 277 10 = 271
ISA-0001	8	This a static value that will be present for all transactions.

4.2.1.4 Supported Clients

NCTracks MFT uses the Ipswitch MoveIT DMZ product as its FTP server. Ipswitch has tested MoveIT DMZ against and fully supports a large number of secure FTP clients using FTP over SSL and SSH. See Appendix A for a complete listing.

Connectivity troubleshooting and/or configuration parameter assistance will be limited with FTP clients. NCTracks does not procure and/or provide licensing for any FTP client. The decision to procure a particular FTP client is the responsibility of the trading partner.

4.2.1.5 Data Exchange Protocols

4.2.1.5.1 SFTP

NCTracks MFTP SFTP uses SSH Protocol 2 and SCP2 only. A client will not be able to connect using only Protocol 1 or SCP (SCP1), and all Terminal sessions will be denied access.

SFTP	
IP Address	12.204.168.65
URL	ftp2.nctracks.nc.gov
Port	22

Exhibit 4-1. SFTP Protocol Information

4.2.1.5.2 FTPS

FTPS requires multiple port numbers during file transfers, as each individual file transfer creates a new connection on a new port.

FTPS	
IP Address	12.204.168.65
URL	ftp2.nctracks.nc.gov
Control Port	990
Data Ports	3000-3003

Exhibit 4-2. FTPS Protocol Information

4.2.1.5.3 FTPES

FTPES requires multiple port numbers during file transfers, as each individual file transfer creates a new connection on a new port.

FTPES	
IP Address	12.204.168.65
URL	ftp2.nctracks.nc.gov
Control Port	21
Data Ports	3000-3003

Exhibit 4-3. FTPES Protocol Information

4.2.1.5.4 HTTPS

Website	
IP	12.204.168.64
URL	www.nctracks.nc.gov/xfr
Port	443
Note: This protocol is accessible only by providers, clearinghouses, service bureaus, and other trading partners that have been provisioned by NCTracks and have valid NCIDs.	

Exhibit 4-4. HTTPS Protocol Information

4.2.1.6 FTP Supported Commands

The NCTracks MFT system supports the following FTP commands.

Command	Comments
USER username	Username indicates the UID to be checked in the NCTracks user database.
PASS password	Password indicates the NCTracks password to be checked in the NCTracks user database.
AUTH type	Starts secure communication for the specified security type: TLS-C or TLS-P.
FEAT	Returns the feature set supported, specifically, AUTH, PROT, and PBSZ.
PROT type	Sets the data connection protection type. For TLS-C security, the PROT command is required to enable security on the data channel.
PBSZ size	Sets the protection buffer size for encryption. Included for compatibility; the size is never checked.
CLNT name version	Sets the FTP client name and version for logging purposes.
LIST	Obtains a directory listing, with date, size, and file name in a format compatible with Microsoft's FTP server. Any command arguments beginning with '-' are ignored.
NLST	Obtains a bare directory listing.
RETR fileID	Downloads a file, first checking that the current user has read access to the file. The fileID can be a complete file name, including an embedded fileID. NCTracks MFT FTP will extract the fileID. When unique file names are enforced for a folder, the file name can be used in place of the ID.
STOR filename	Uploads a file. The NCTracks MFT system will create a new fileID and return it in the 226 response.
APPE filename	Appends a file. This command is supported only for resuming file transfers. The NCTracks MFT system will create a new fileID, copy the old partial file and append new data, and return it in the 226 response.
CD ~	Changes current directory to the user's default (not home) directory.
CWD directory	Changes current directory. See below.
MKD directory	Creates a directory, if the user has permission to do so.
RMD directory	Deletes a directory, if the user has permission to do so.
DELE fileID	Deletes the file, if the user has permission to delete it.

Command	Comments
RNFR fileID	Changes the original file name associated with a fileID, if the user has permission to modify it.
RNTO filename	Changes the original file name associated with a fileID, if the user has permission to modify it.
REST skipcount	Sets the byte skip count for a subsequent RETR or STOR command. For RETR, the NCTracks MFT system will skip the first “skipcount” number of bytes in the downloaded file. For STOR, the NCTracks MFT system will copy the first “skipcount” number of bytes from the destination file to a new file and then append the transmitted bytes.
SIZE filename	Reports the size in bytes of the named file, the same number returned in a directory list.
MODE type	Sets the mode in which data is to be transferred via the data connection: S for Stream Mode or Z for Zip compression mode.
SYST	Reports the system type. The returned string indicates compatibility with the Microsoft Windows FTP server.
HELP	Displays a list of commands.
PORT	Initiates an active data connection. **Note**: The NCTracks MFT system is configured to allow only passive connections; this command will be refused.
PASV	Initiates a passive connection. This command is used by some FTP clients to accommodate firewalls that do not allow an FTP server to initiate TCP data connections.
QUIT	Quits the session.

Exhibit 4-5. FTP Commands

4.2.1.7 FTP Integrity Check Commands

NCTracks MFT FTP supports the following commands for the purposes of integrity checking:

Command	Comments
INTEGRITY type	Enables integrity checking on STOR and RETR. For type L, use “lump mode” data stream, which compresses data on the fly, and include an SHA1 hash of the file for integrity verification. For type H, “hash mode,” the data stream is standard, and the client is responsible for checking the SHA1 hash for integrity verification. Type N turns integrity checking off.
XSHA1 filename	Returns the SHA1 hash of the file named, usually the most recently transferred file.
HASH OK/BAD	Notifies NCTracks MFT FTP, after a STOR or RETR, that the client has verified the file SHA1.

Exhibit 4-6. FTP Integrity Check Commands

4.2.1.8 FTP Nontraditional Commands and Unsupported Commands

NCTracks MFT FTP supports the following commands in a nontraditional way.

Command	Comments
TYPE I or A	Implements the ASCII and binary commands. Not supported; all transfers are binary. (In other words, NCTracks MFT DMZ does not automatically add/strip carriage returns or perform other character manipulation.) Contact NCTracks support if this is a concern.

Exhibit 4-7. FTP Nontraditional Commands

NCTracks MFT FTP does not support the following commands:

- ACCT
- SMNT
- REIN
- STOU

- ALLO
- ABOR
- SITE

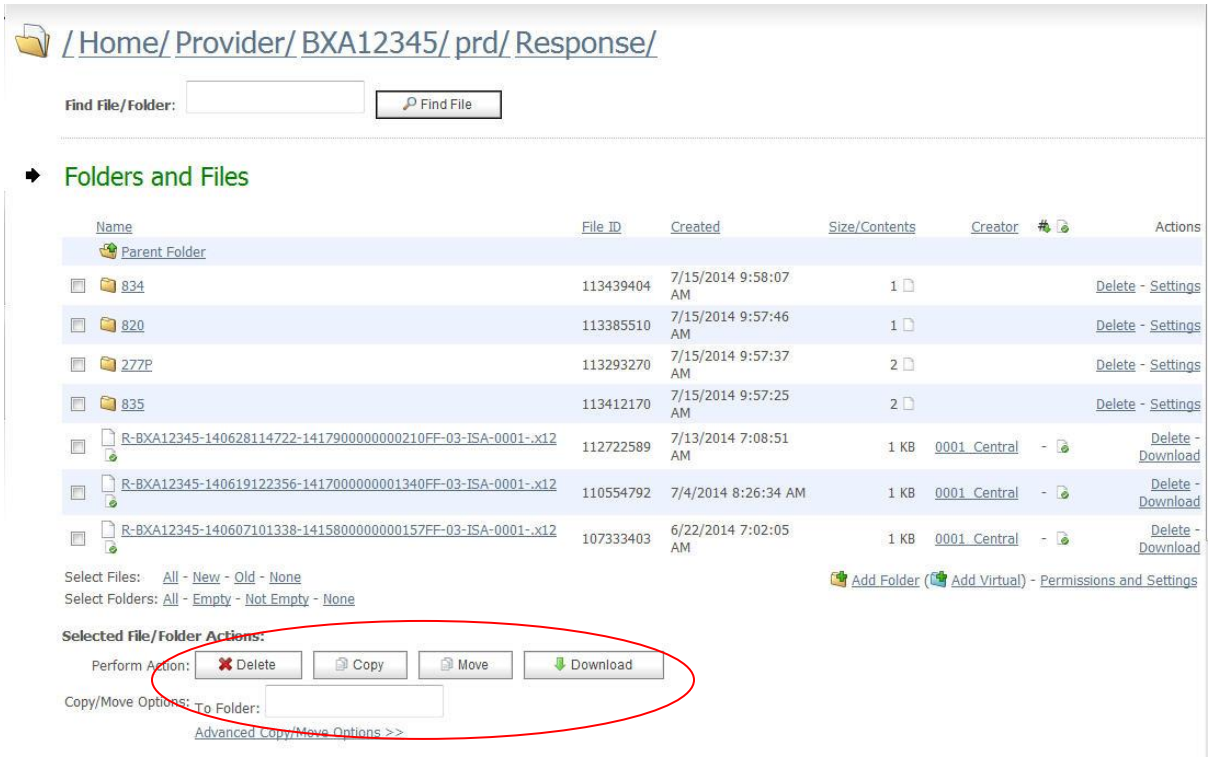
4.2.1.9 Directory View Differences Between Browser Session and FTP Session

Each user's "default folder" is their mailbox. When using FTPS or SFTP, the user's default folder, also known as the mailbox folder, will become their root folder when they sign on through the FTPS or SFTP interfaces. The only files and folders the user will be able to see in the default folder will be those transactions that are provisioned to the user (if the user is not provisioned for a transaction, they will not see that folder in their mailbox). Users have permission to copy, move, download, and delete files; these options are located at the bottom of the Response screen. **Please remember to download the file before deleting.** Contact EDI Technical Assistance if a file is deleted in error (refer to Section 2.1, Working Together for contact information).

In the following examples, the same directory structure is shown as is seen via a browser and a secure FTP session. Users can retrieve outbound transactions from the Response folder. The 999, TA1, F-File, 271, and 277 will be located inside the Response folder. Also, within the Response folder, there will be subfolders for 835, 277P, 820, and 834O (not all users will have all the folders listed in the following example).

Browser Session
/[mailbox]/[env1]/in

Secure FTP Session
/env1]/in



4.2.2 NCTracks Provider Portal – Batch X12 Submissions

NCTracks provides a web-based application that is customized to allow the entry and submission of all 5010 NCTracks inbound X12 transactions.

The requirements for using the Provider portal include:

- A TSN and Certification Statement, which should be obtained prior to enrollment
- Internet Explorer 8 and above or compatible browser
- Internet browser that supports 128-bit encryption and cookies
- Minimum connection speed of 56K
- An accessible email address

The following transactions can be submitted and corresponding responses presented through the NCTracks Provider portal:

- 270/271 – Eligibility Benefit Inquiry and Response
- 276/277 – Claim Status Request and Response
- 837 – Dental, Professional, and Institutional Claims
- 834I – Benefit Enrollment and Maintenance

This feature allows Trading Partners to submit an X12 batch file that contains inbound transactions. Trading Partners will be given a menu option to submit batch EDI transmissions through the Provider portal as shown below. The MoveIT system is an FTP and Web hybrid that supports Web browsers and secure FTP clients for the secure submission of batch files over encrypted connections using the HTTPS, FTPS, or SFTP protocols.

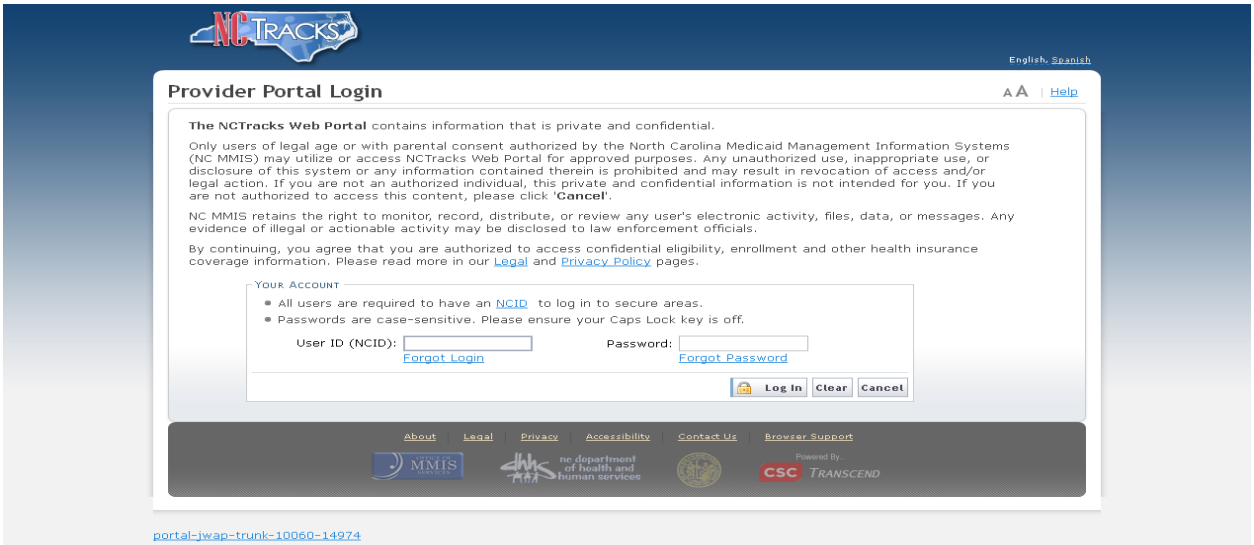
When this functionality is used, the transactions will be processed in batch mode and not real time. The TA1, F-File, and 999 responses to these batch transactions will vary based on the transaction volume per file, First In First Out (FIFO), system/CPU load, and other NCTracks processing priorities.

Steps for Batch Submissions Through the NCTracks Portal

Step 1:

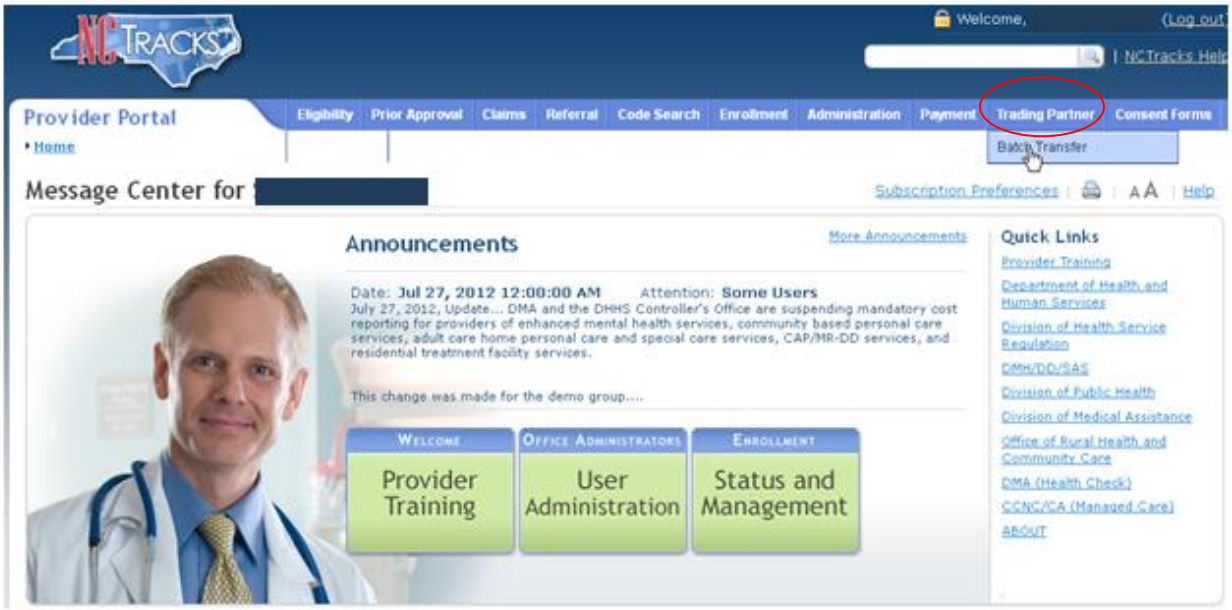
Log in to https://www.nctracks.nc.gov.

Enter your NCID and Password and click the **Log In** button.

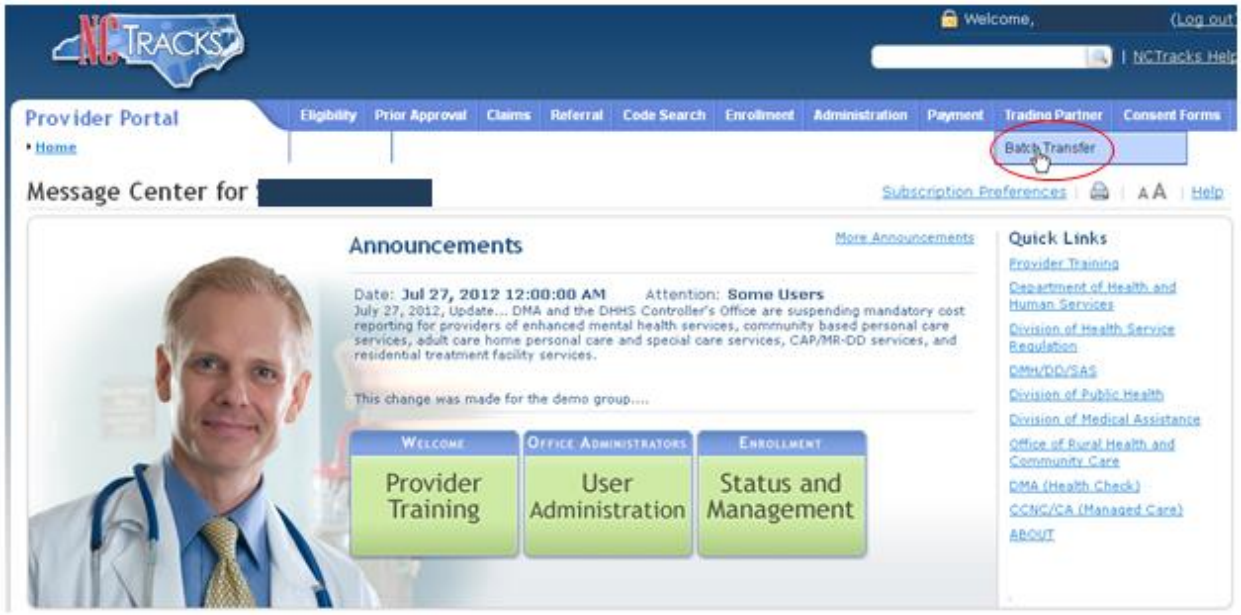


Step 2:
Select the **Providers** option.

Step 3:
Select the **Trading Partner** option.

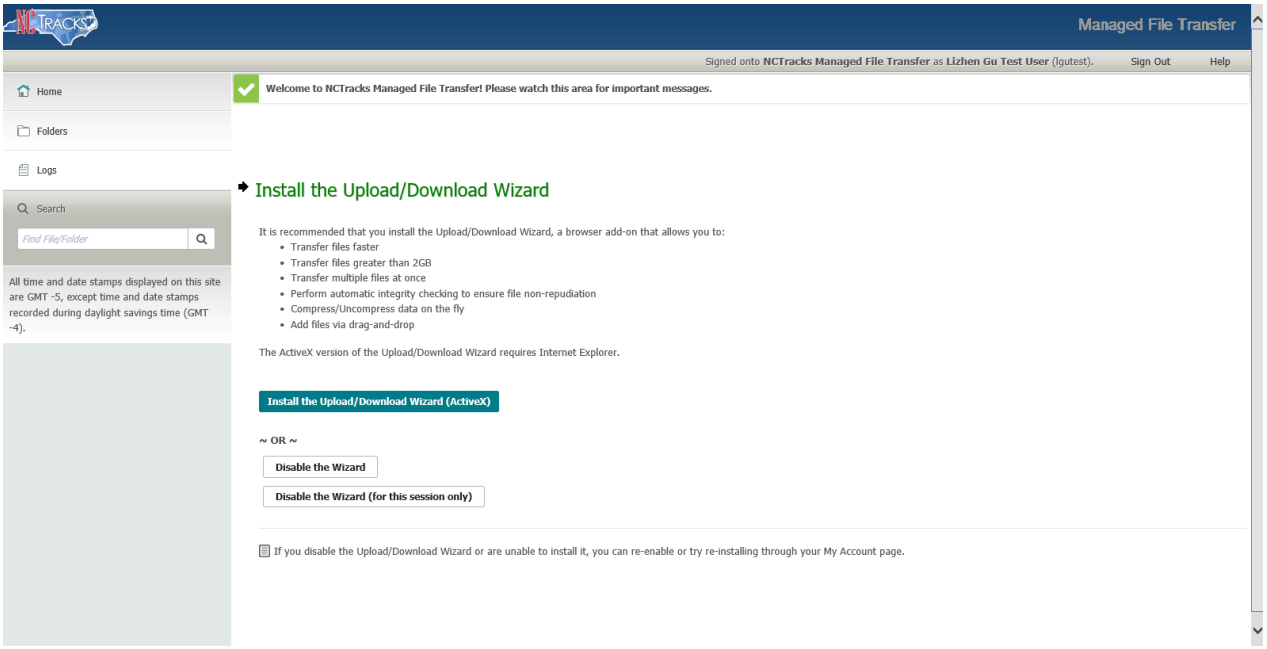


Step 4:
Select the **Batch Transfer** option.



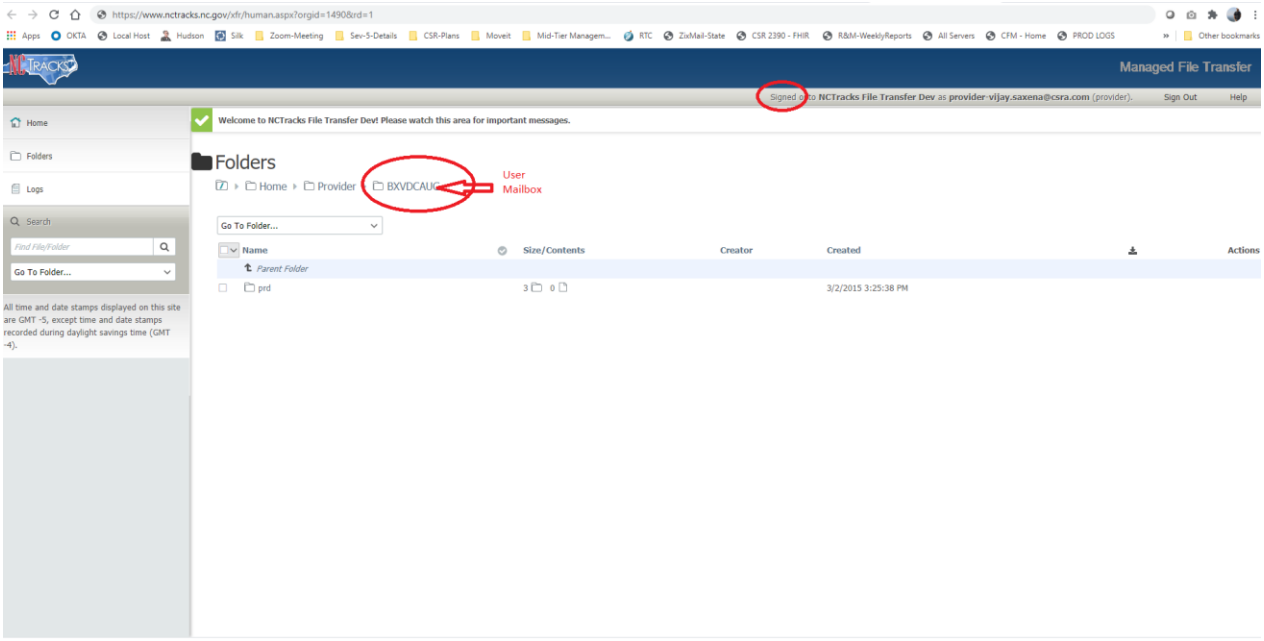
Step 5:

This step will take users to the MoveIT tool, which manages file transfers. For information on installation of the Upload/Download Wizard, refer to Appendix B.



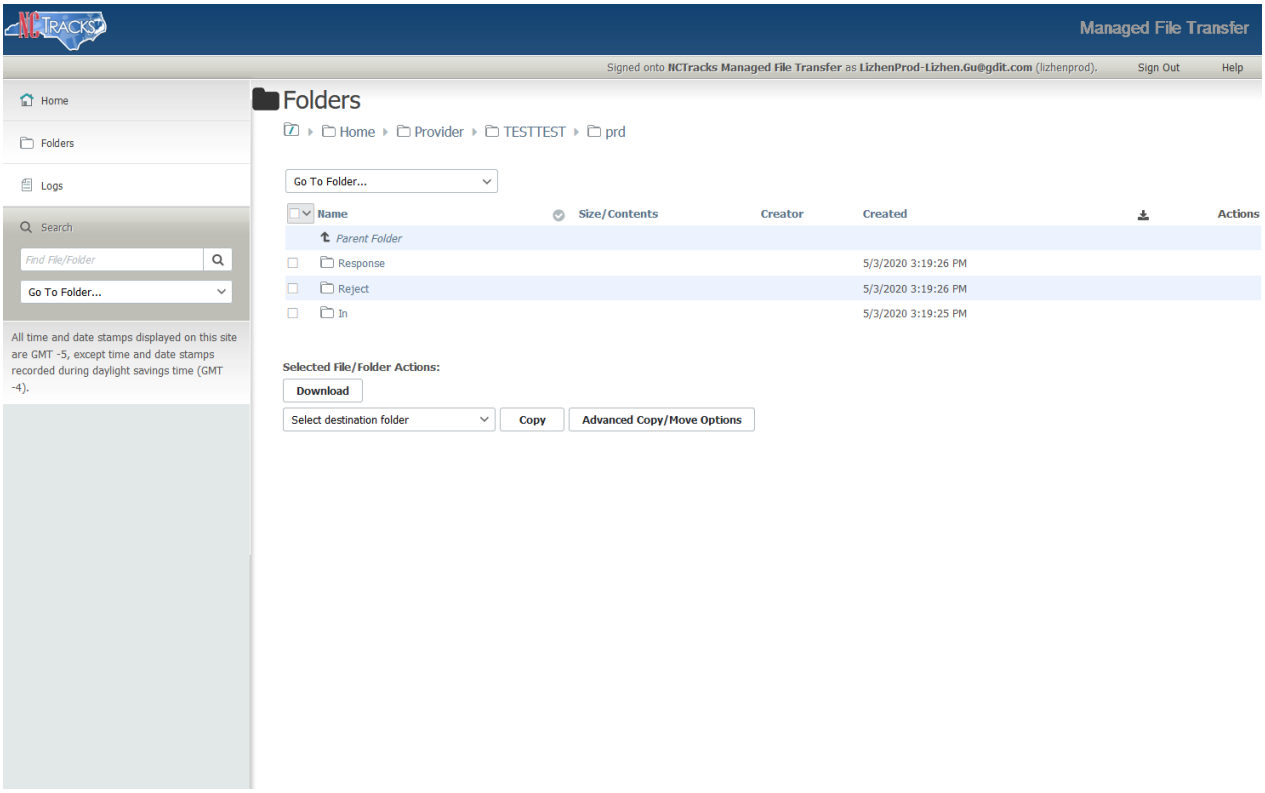
Step 6:

Click the **Home** button to go to the Trading Partner's mailbox.

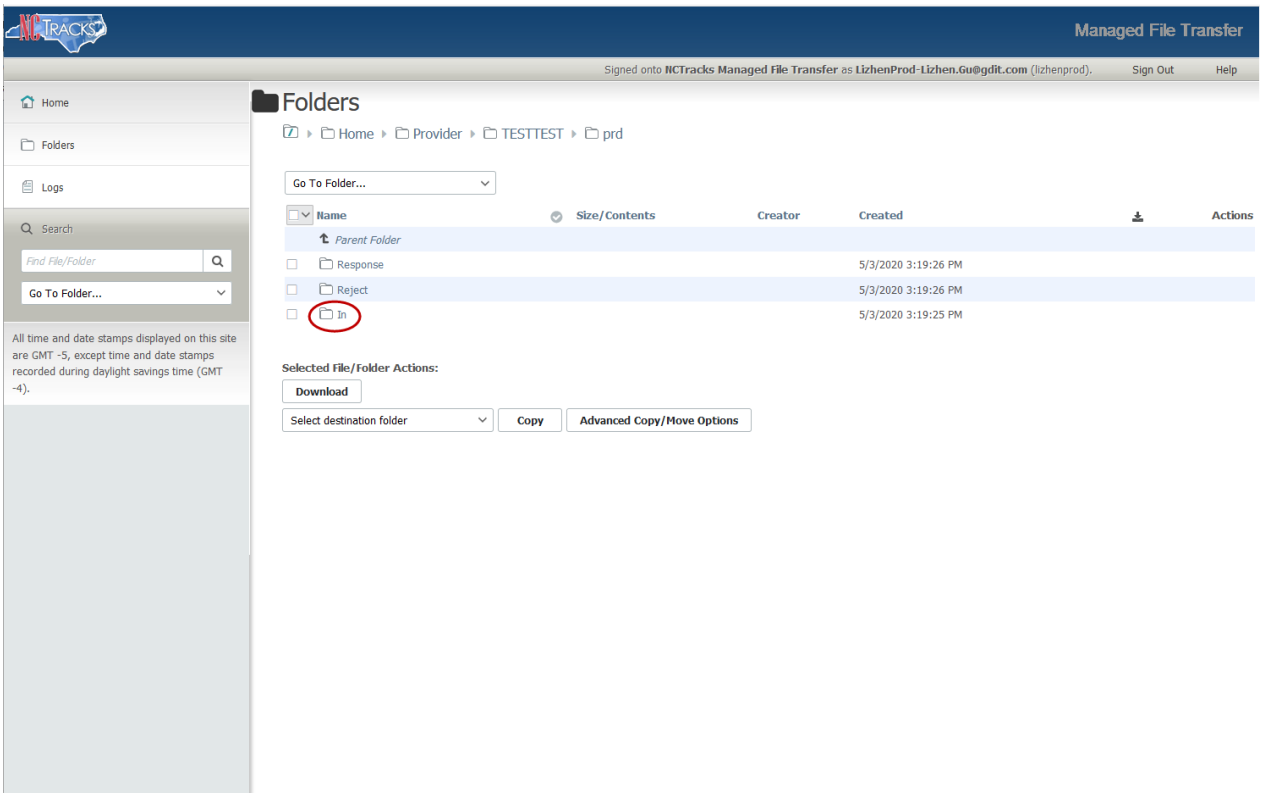


Step 7:
This step involves the following three folders:

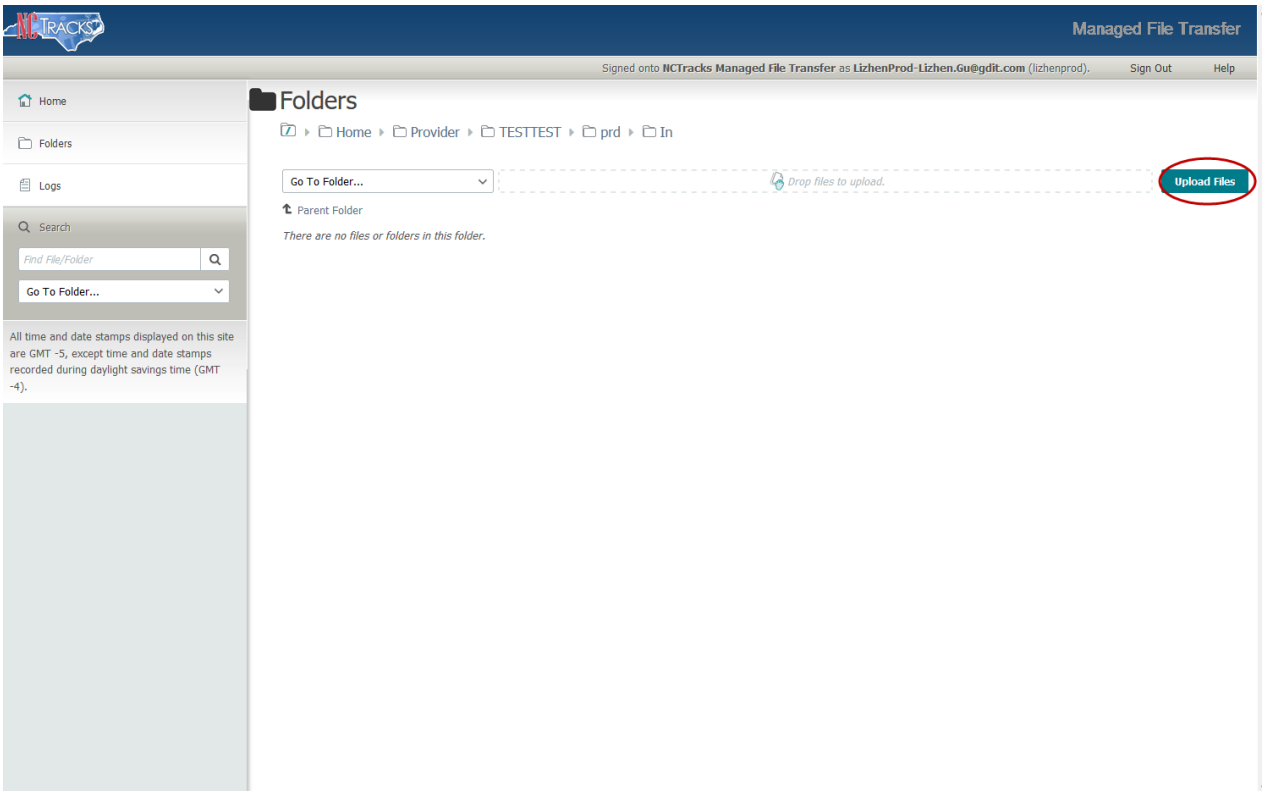
- **In** – Users will drop or upload the X12 inbound transactions into this folder (270, 837, 276, 834I).
- **Response** – Users can retrieve outbound transactions from this folder. The 999, TA1, F-File, 271, and 277 will be located inside the Response folder. Within the Response folder, there will also be subfolders for 835, 277P, 820, and 834O.
- **Reject** – This folder contains any files that did not follow certain naming rules, zip files, and files with invalid extensions as outlined in Section 4.2.1.3, File Naming Standards.



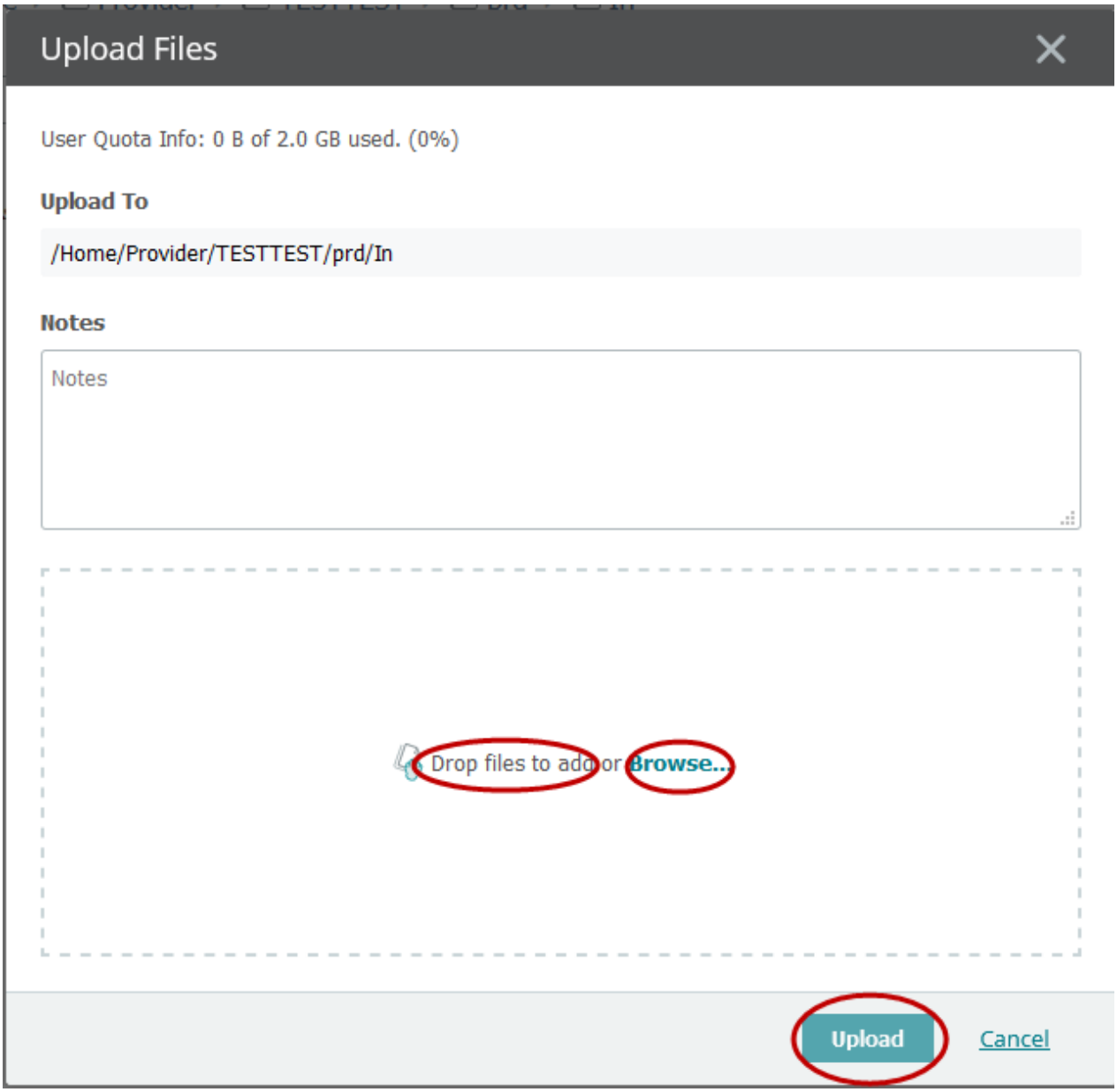
Step 8:
Click the “In” hyperlink for uploading an X12 file.

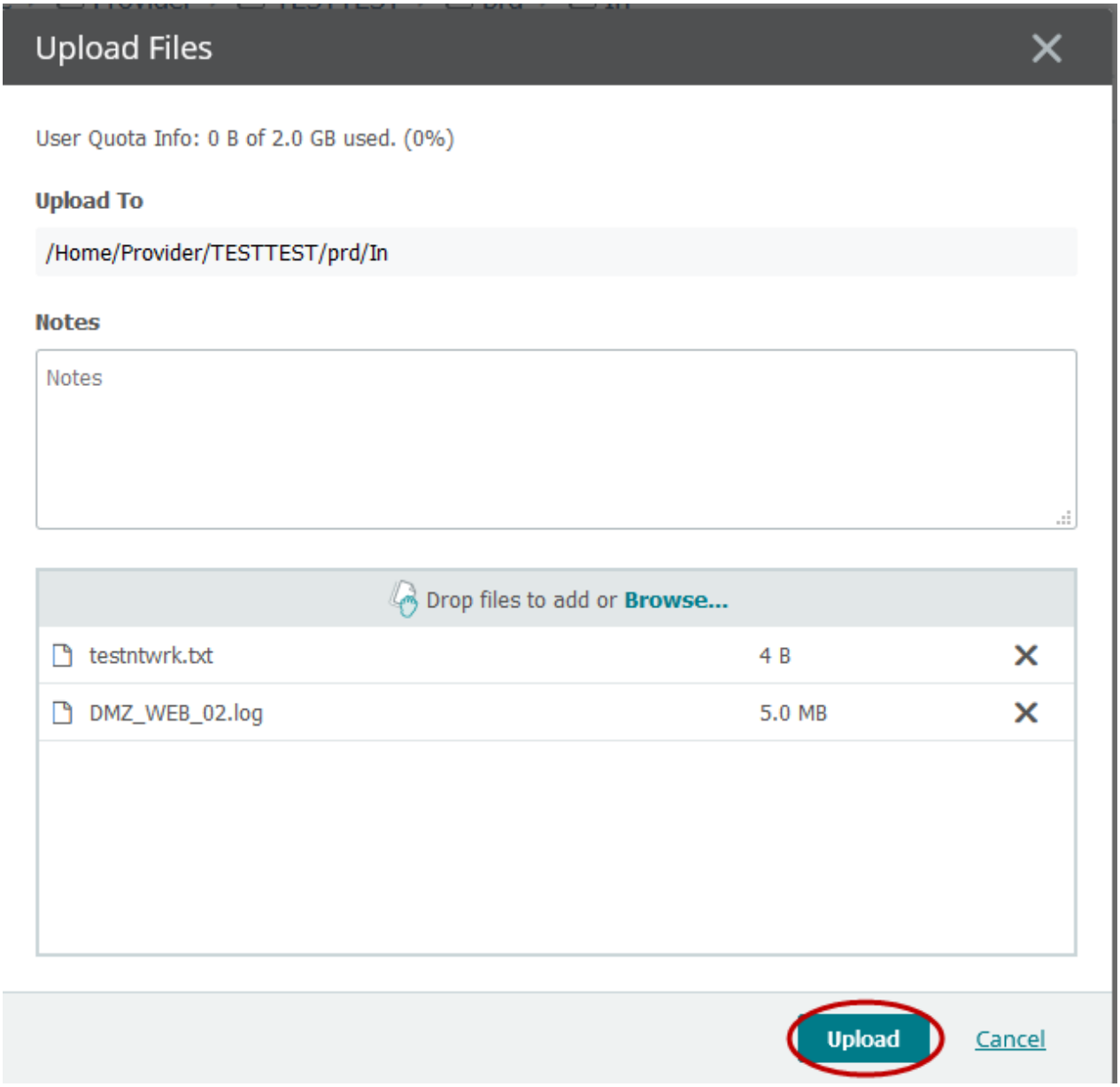


Step 9:
Click the “Upload Files” button.



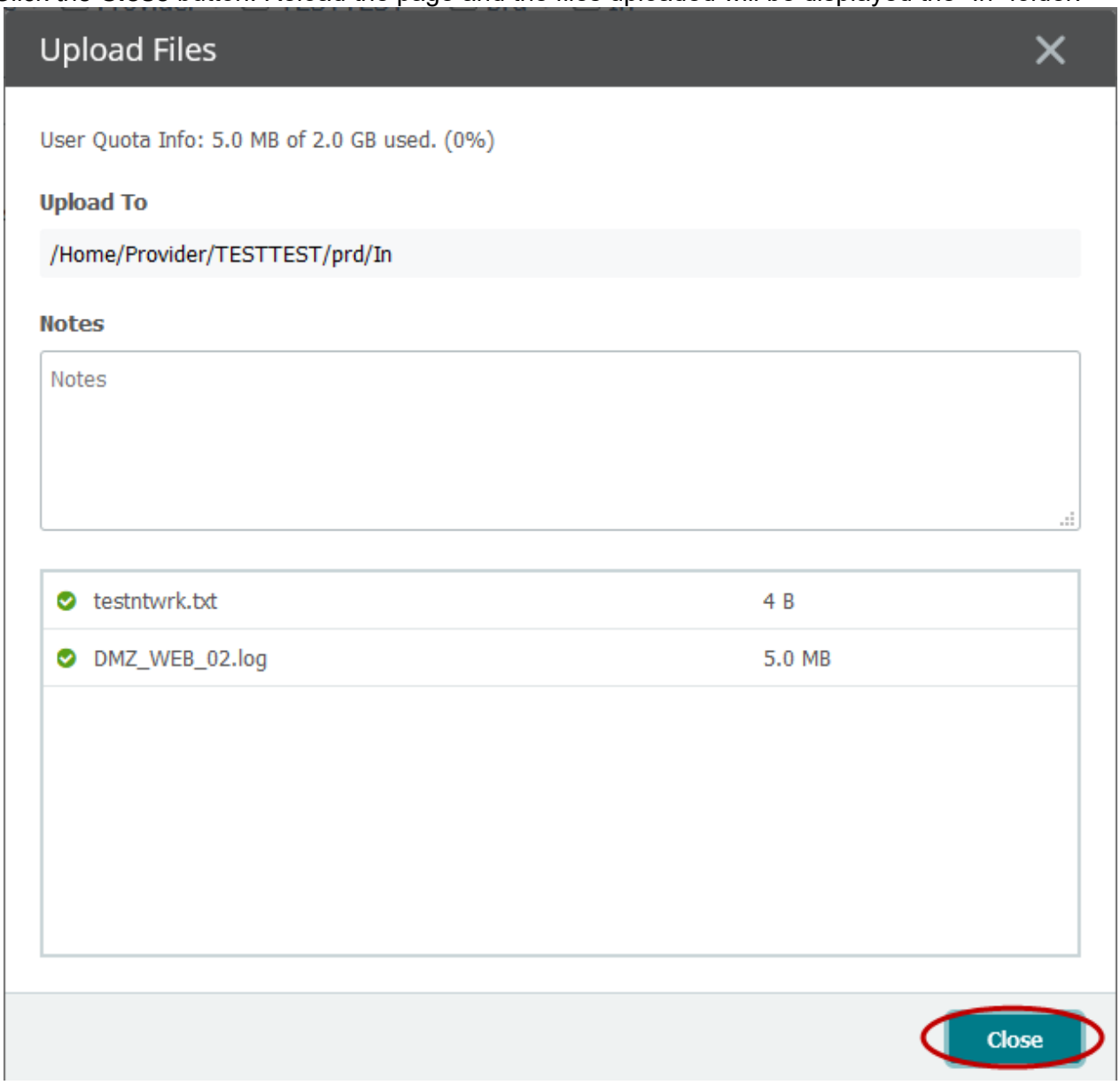
Drag and drop the file(s) to the “Drop files” area, or click Browse link to locate the files to be uploaded, then click Upload button to upload file(s)


Upload Files
User Quota Info: 0 B of 2.0 GB used. (0%)
Upload To
/Home/Provider/TESTTEST/prd/In
Notes
Notes
Drop files to add or Browse...
Upload
Cancel


Upload Files
User Quota Info: 0 B of 2.0 GB used. (0%)
Upload To
/Home/Provider/TESTTEST/prd/In
Notes
Notes
Drop files to add or Browse...
testntwrk.txt
4 B
DMZ_WEB_02.log
5.0 MB
Upload
Cancel

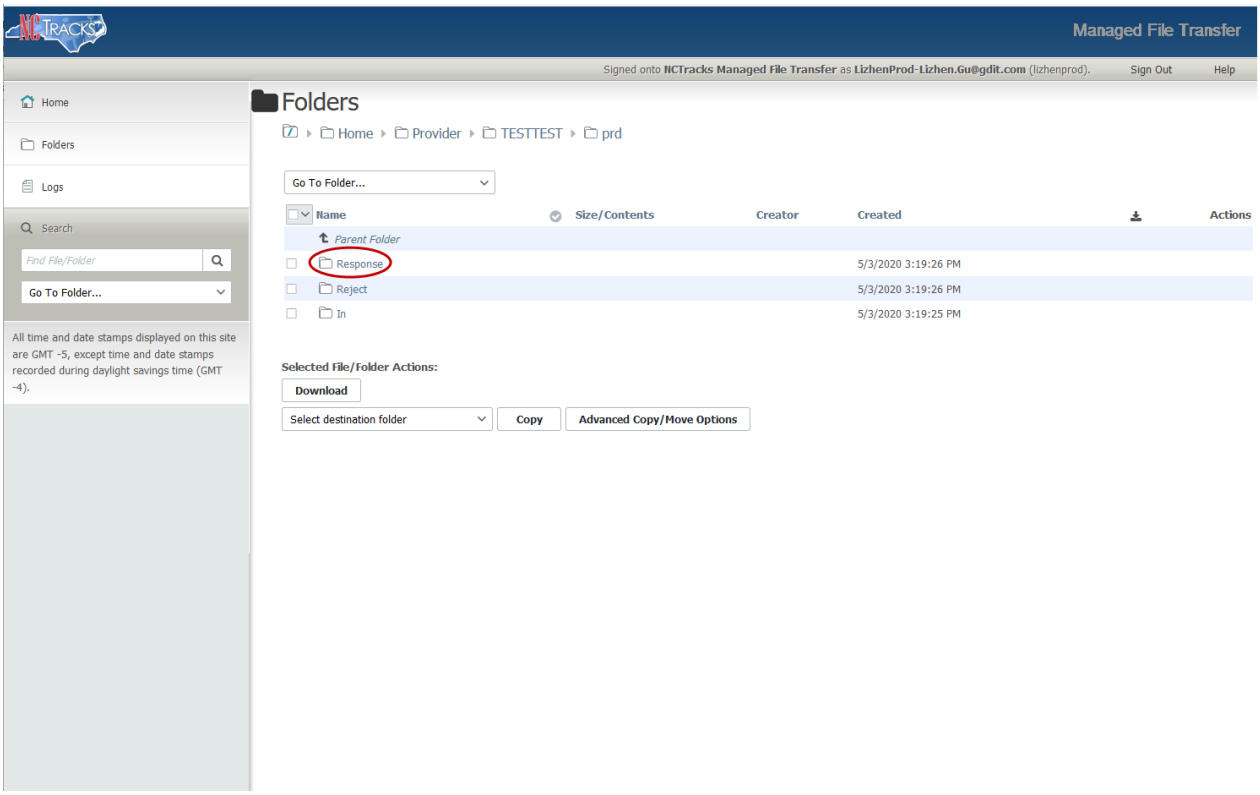
Step 10:

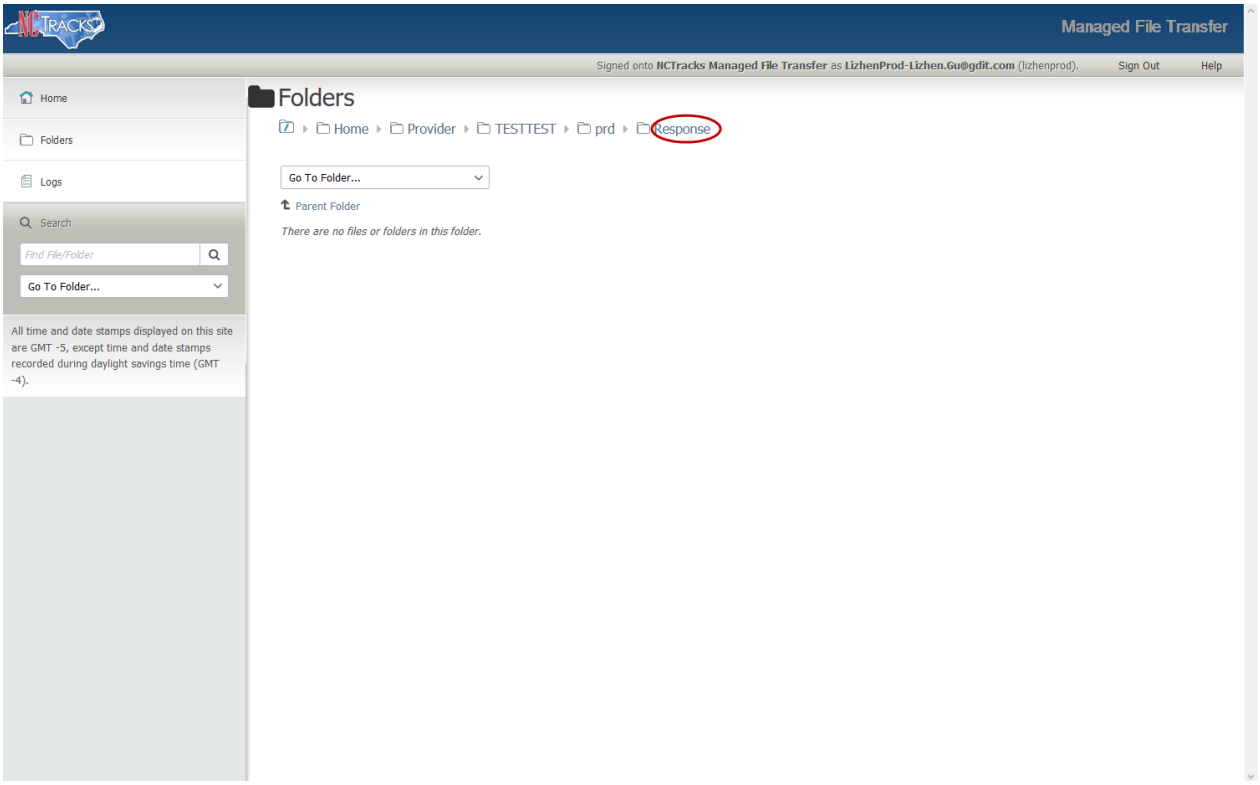
Click the **Close** button. Reload the page and the files uploaded will be displayed the “In” folder.



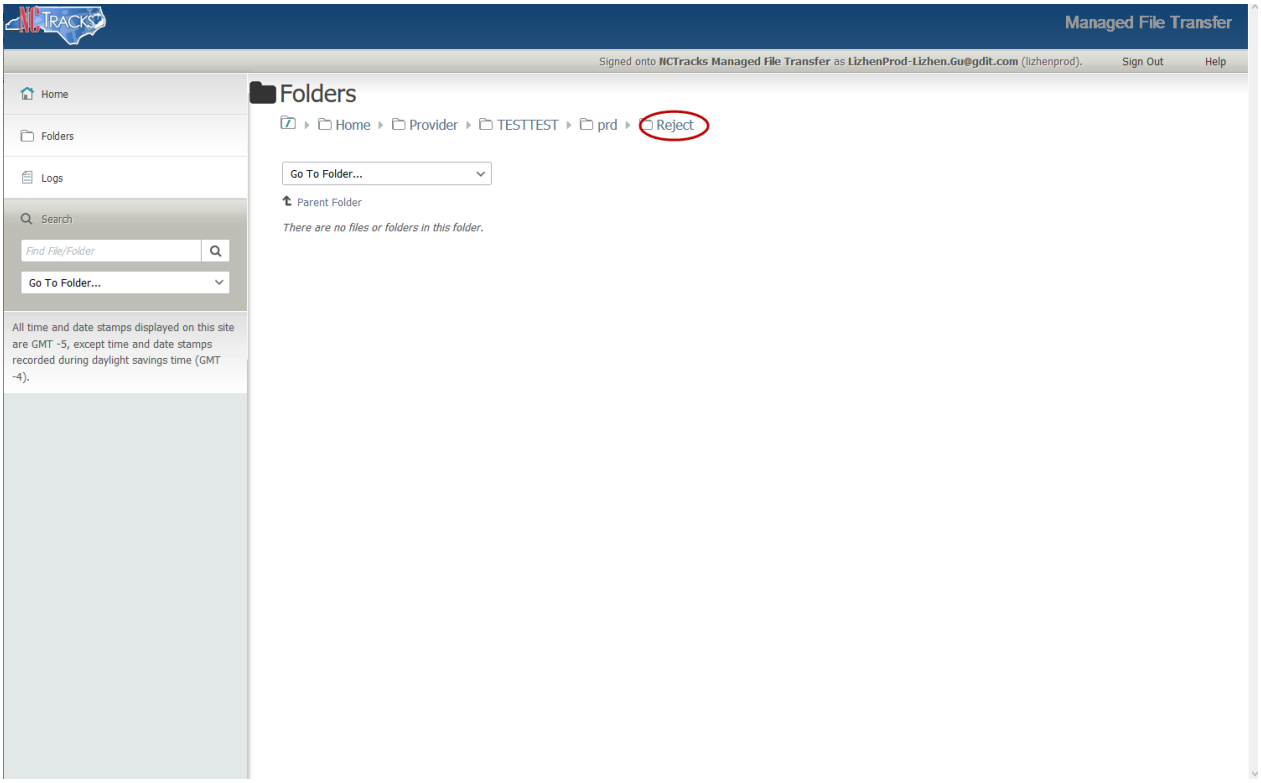
Step 11:

Click the “Response” hyperlink to view/download any outbound transactions such as 835, 820, 999, TA1, F-File, etc. The 835, 277P, 820, and 834O transactions are subfolders within the Response folder. All other transactions, such as the 999, TA1, F-File, 271, and 277 files, will be located inside the Response folder.




Managed File Transfer
Signed onto NCTracks Managed File Transfer as LizhenProd-Lizhen.Gu@gdit.com (lizhenprod).
Sign Out
Help
Home
Folders
Logs
Search
Find File/Folder
Go To Folder...
All time and date stamps displayed on this site are GMT -5, except time and date stamps recorded during daylight savings time (GMT -4).
Folders
Home
Provider
TESTTEST
prd
Response
Go To Folder...
Parent Folder
There are no files or folders in this folder.

Step 12:
Click the “Reject” link to view/download any files that may have been rejected.



4.2.3 CPU-to-CPU Real Time

This method consists of a direct connection established between the submitter and the processor. It is most suitable for submitters exchanging substantially large transaction volumes with NCTracks.

Data is exchanged as request/response pairs in a synchronous fashion, meaning:

- Over an established, otherwise idle connection, the vendor sends a single request, then waits for NCTracks to process that request and reply with a single response.
- After a request/response pair has completed (not before), another request/response pair may be communicated over the same connection.
- Such synchronous communications may continue as long as there is traffic to send or until the connection is dropped.
- Multiple concurrent connections (i.e., up to a prearranged limit) are allowed, each adhering to the requirement for strictly synchronous communications.
- The requirement for synchronous communications implies that TCP/IP writes to NCTracks must be synchronized with TCP/IP reads of the corresponding responses from NCTracks. Correlation numbers are not required and are not included in the interface.

Each request and its associated response are separately formatted for reliable network transfer in communication wrappers as follows:

- STX 1 byte (0x02)
- byte count 8 bytes, leading zeros, inclusive of wrapper (payload length + 18)
- reserved 8 bytes, all zeros (required and reserved for future use)
- payload (e.g., HIPAA request or response)
- ETX 1 byte (0x03)

TCP/IP connection drops should be rare, but they can be expected to occur under some circumstances.

- For security and performance reasons, NCTracks uses an idle connection timer that will forcibly close a connection that has been idle for at least 20 minutes.
- If the NCTracks end of a connection experiences a condition where it cannot continue, it will terminate the connection abruptly. For example, the connection will terminate if the amount of data read from the TCP/IP interface is greater than the value specified in the byte count field of the required message wrapper.
- The side that originates connections to NCTracks is expected to handle abrupt disconnects. Typically, when a connection is lost for any reason, the vendor side should simply establish a new connection, either immediately or when there is traffic to send.
- Normally, the first or second attempt to connect will succeed. A brief interval of at least 3 seconds must be included between successive connection attempts. In the event of significant hardware failure, it may take 5 – 10 minutes before new connection attempts will succeed.
- After a new connection is established, continue processing by resubmitting a request or proceeding to the next request, as appropriate.

There are three possible responses to each request submitted over an established connection:

1. A single-character negative acknowledge (NAK) (0x15) signals that a request was received but the wrapper was invalid. For example, no STX was detected.
2. A complete response formatted as the payload in the required communication wrapper. Specific responses should be discussed during vendor testing with NCTracks, before production deployment.
3. Disconnect (connection lost) at any point, as described above.

4.2.4 NCTracks Provider Portal – Direct Data Entry

NCTracks provides a real-time web-based application that is customized to allow the entry and submission of specific transactions, including the 837 and D.0 transactions.

The requirements for using the Provider portal include:

- A TSN and Certification Statement, which should be obtained prior to enrollment
- Internet Explorer 8 and above or compatible browser
- Internet browser that supports 128-bit encryption and cookies
- Minimum connection speed of 56K
- An accessible email address

The following transactions can be submitted and corresponding responses presented through the NCTracks Provider portal:

- 270/271 – Eligibility Benefit Inquiry and Response
- 276/277 – Claim Status Request and Response
- 837 – Dental, Professional, and Institutional Claims
- D.0 – B1, B2, B3, E1, N1, N2, N3

The Provider portal features the real-time claim submission functionality under the 837 Dental, Professional, and Institutional transactions, as well as NCPDP pharmacy, which allows real-time adjudication of the claim. When this functionality is used, a claim adjudication status response is sent to the submitter shortly after submission. Please visit the following NCTracks portal website, using your NCID and password, to submit the real-time direct data entry of transactions:

https://www.nctracks.nc.gov

4.2.5 CAQH-CORE Phase II Connectivity (270/271 and 276/277)

Overview

NCTracks supports CAQH-CORE Phase II compliant Simple Object Access Protocol (SOAP) and Multipurpose Internet Mail Extensions (MIME) interfaces that allow Trading Partners to programmatically submit Batch and Real-time 005010X279A1 270 Eligibility or Benefit Inquiry and 005010X212 276 Claims Status Request transactions. Trading Partners are also allowed to programmatically request and submit 005010X231A1 TA1/999 Implementation Acknowledgment for Health Care Insurance and batch 005010X279A1 271 Eligibility or Benefit Response and 005010X212 276 Claims Status Response transactions. Refer to Section 4.2.7, CAQH-CORE Phase II and III – Submitting 999 Transactions, to submit a batch 999 to NCTracks. Additional information about the Phase II interface can be found at http://www.caqh.org/CORE_phase2.php.

User Requirements

Users are required to be active Trading Partners and have a valid TSN and NCID. For Trading Partner enrollment information, refer to Section 2.2.1, Trading Partner/Providers Enrollment. The Trading Partner must also be provisioned to submit using the CAQH-CORE Phase II methodology. For user provisioning for CAQH-CORE, refer to Section 2.2.2.3, User Role Setup Instructions.

Software Requirements

NCTracks does not provide software for SOAP or MIME connectivity. Trading Partners must obtain their own software for submittal. NCTracks requires version 2.2.0 for SOAP and MIME clients. Most programming languages support SOAP and MIME clients and contain documentation to help Trading Partners create a client that can send/receive information to this interface. Sample 270, 271, and 999 Request SOAP and MIME clients are included in Appendices C, D, and E, respectively. A sample 999 Submission SOAP and MIME client is included in Appendix H. The samples of SOAP and MIME are only examples, and are not intended to function as-is.

The Trading Partner will need to understand how to write the program and handle the response appropriately. Follow the CORE II specifications described above, which contain detailed instructions about the format of the request and the response.

For more information pertaining to CORE Phase II requirements and SOAP and MIME submissions, please refer to the following websites:

- CORE Phase II: http://www.caqh.org/CORE_phase2.php
- SOAP: http://www.w3.org/TR/soap/
- MIME Multipart: http://www.w3.org/Protocols/rfc1341/7_2_Multipart.html

CAQH-CORE Production
NCTracks will not provide ongoing testing for SOAP and MIME connectivity. Refer to Section 4.2.5.1, SOAP Attributes and MIME Attributes for 270/271 and 276/277 for production file setup instructions.

Production files should be submitted to the following URL:

https://edi.nctracks.nc.gov/EDIGateway

CORE Interface Parameters
The CORE interface requires submission of certain parameters. The following sections describe specific information for SOAP and MIME submissions and the expectations of NCTracks.

4.2.5.1 SOAP and MIME Attributes for 270/271 and 276/277

PayloadType
The Trading Partner must submit one of the following Payload types:

- X12_270_Request_005010X279A1
- X12_276_Request_005010X212
- X12_999_RetrievalRequest_005010X231A1
- X12_TA1_RetrievalRequest_005010X231A1
- X12_005010_Request_Batch_Results_271
- X12_005010_Request_Batch_Results_277

ProcessingMode
The Trading Partner must submit either Batch or RealTime.

PayloadID
The PayloadID is used to link request and response files. A unique ID specific to an NCID should be used that will help identify the response to a submitted request, and the PayloadID should not be duplicated (see the naming standards in the Payload description below). Note that only one PayloadID per message can be used. The PayloadID should be in the International Standards Organization (ISO) UUID format. Please refer to the XSD and WSDL version 2.2.0, located on the CAQH-CORE website at http://www.caqh.org/SOAP/WSDL/.

PayloadLength
The PayloadLength is for Batch submissions only and should be determined by the Trading Partner.

TimeStamp
The format of the TimeStamp must follow the conventions found at http://www.w3.org/TR/xmlschema11-2/#dateTime.

An example of a valid TimeStamp is 2014-02-01T10:30:55-00:00.

SenderID
The SenderID should identify the sender. It can be up to 50 alphanumeric characters and cannot contain spaces.

ReceiverID
Must contain “NCTracks”.

CORERuleVersion
Must contain “2.2.0”.

CheckSum
NCTracks requires the SHA-1 digest for the Payload only calculation for the CheckSum. For CheckSum naming standards, please refer to the XSD and WSDL, version 2.2.0, located on the CAQH-CORE website at http://www.caqh.org/SOAP/WSDL/.

Payload
For RealTime submissions, the Payload contains the ASC X12 data for the submission. The ASC X12 file must be valid with the correct settings in the envelope. For the correct settings and NCTracks rules, refer to the appropriate Companion Guide for the submission, located at https://www.nctracks.nc.gov/content/public/providers/provider-trading-partners.html.

For Batch submissions, the Payload contains the name of the ASC X12 batch file, and the file should be submitted as an attachment. The ASC X12 file must be valid with the correct settings in the envelope. For the correct settings and NCTracks rules, refer to the appropriate Companion Guide for the submission, located at https://www.nctracks.nc.gov/content/public/providers/provider-trading-partners.html.

File Naming Standards for X12 Inbound Transactions
The ASC X12 file must adhere to the following naming standards:

- File extensions not accepted:

  *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd, *.pif, *.pot, *.reg, *.scr, *.sct, *.shb, *.shs, *.sys, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh, *.zip
- Special characters (for example, hyphen, asterisk, question mark) are not allowed in file names.
- Zip files are not allowed for SOAP transmittals.

Error Handling
The Trading Partner may receive an error if attributes are entered incorrectly and will receive an appropriate error message based on the error created. Refer to Section 4.2.8, SOAP and MIME Error Messages, for possible error messages.

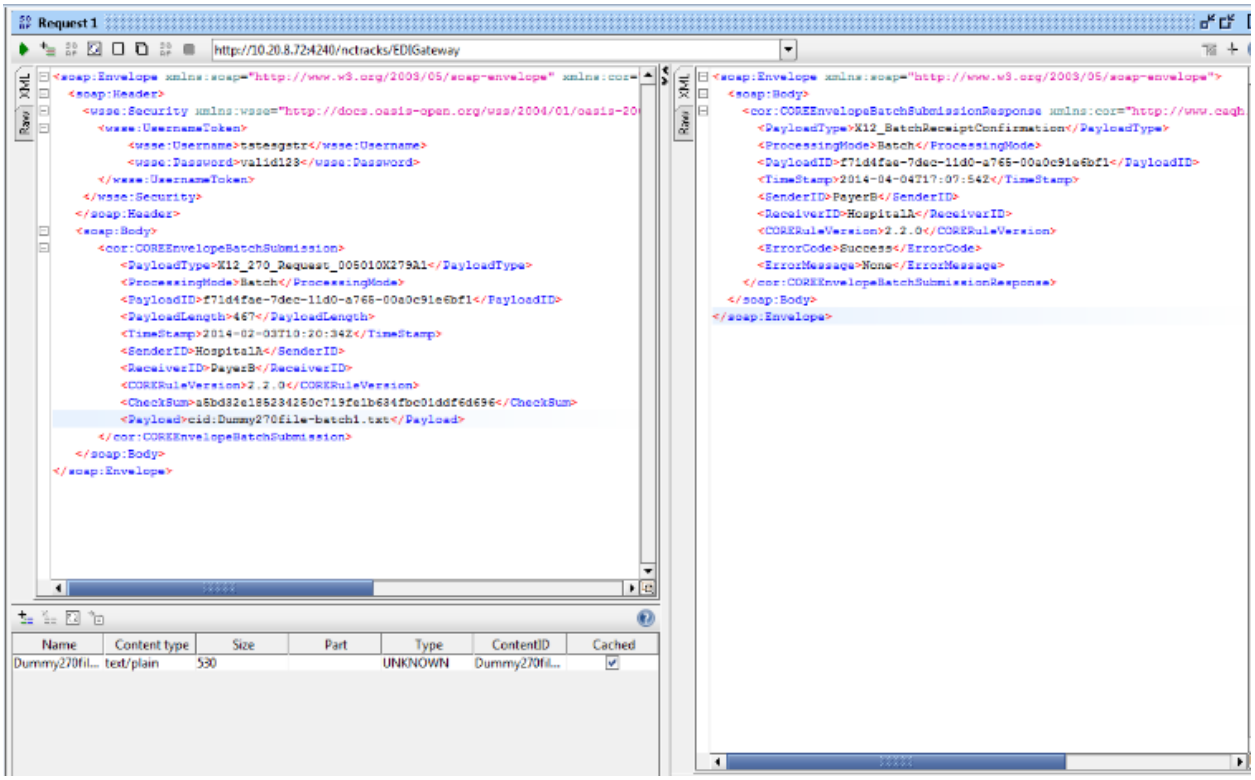
4.2.5.2 SOAP for 270/271 and 276/277

NCTracks has the following submission types for SOAP transmittal. The following screenshots are examples only. Sample 270, 271, and 999 Request SOAP and MIME clients are included in Appendices C, D, and E, respectively. A sample 999 Submission SOAP and MIME client is included in Appendix H.

Batch Submission

- Users can submit a Batch 270 or 276 SOAP with multiple requests.
- A Batch Results Retrieval Request is used to request a 271 or 277 response for a submitted 270 or 276.

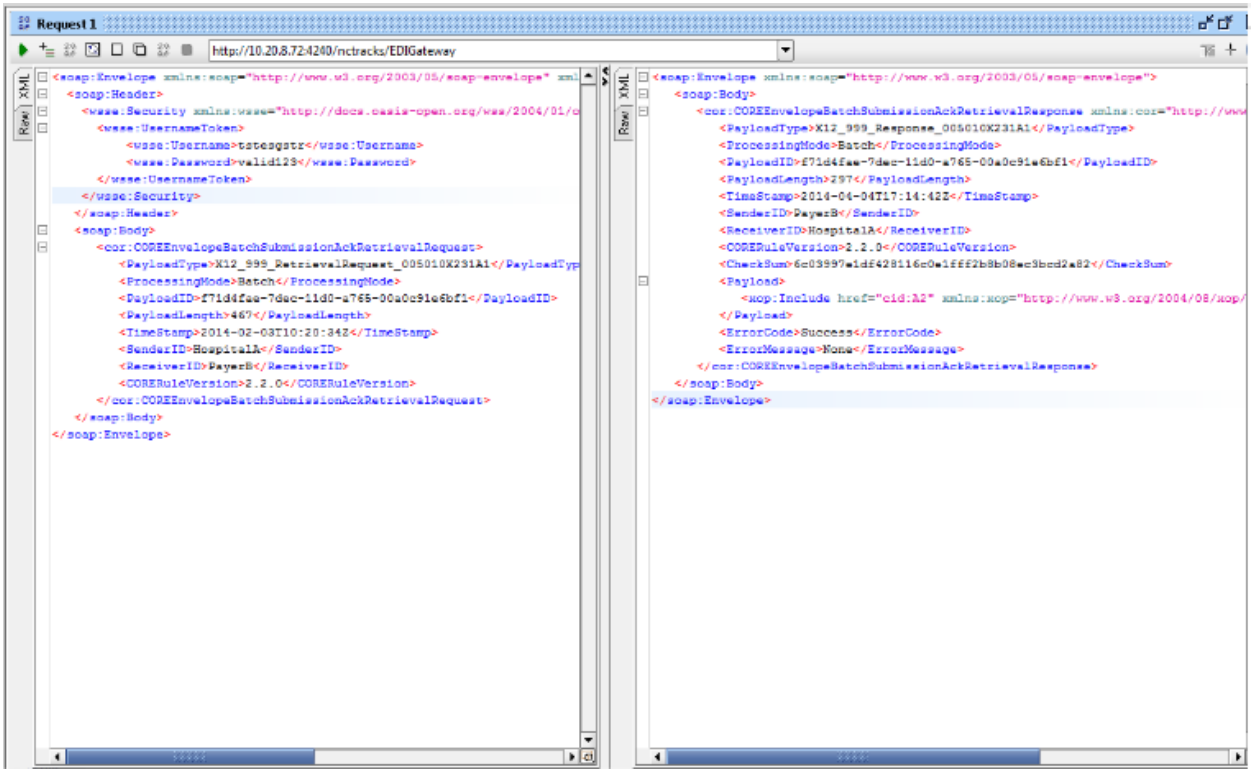
Example of a Batch Submission and Response:



Batch Submission Acknowledgment Retrieval Request

Users can request the X12 999 Acknowledgment for a 270 or 276 submission.

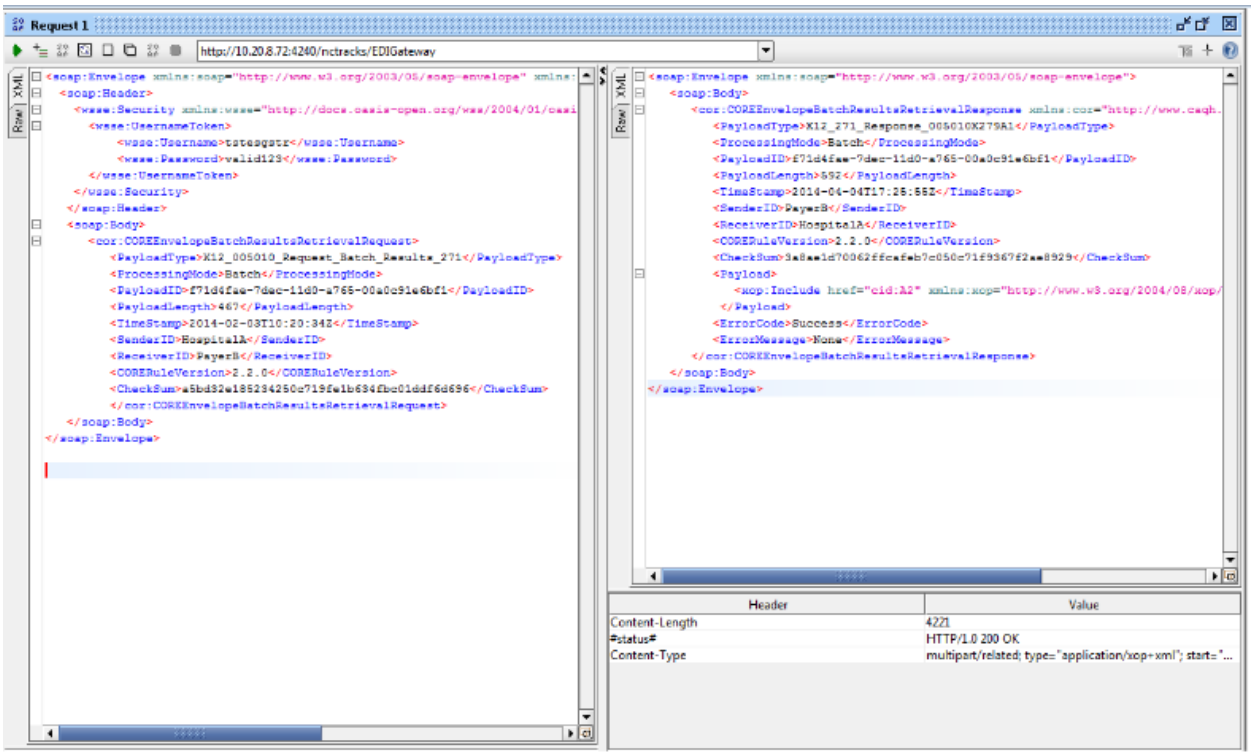
Example of a Batch Submission Acknowledgment Retrieval Request and Response:



Batch Results Retrieval Request

Users can request the 271 or 277 responses for a 270 or 276 request.

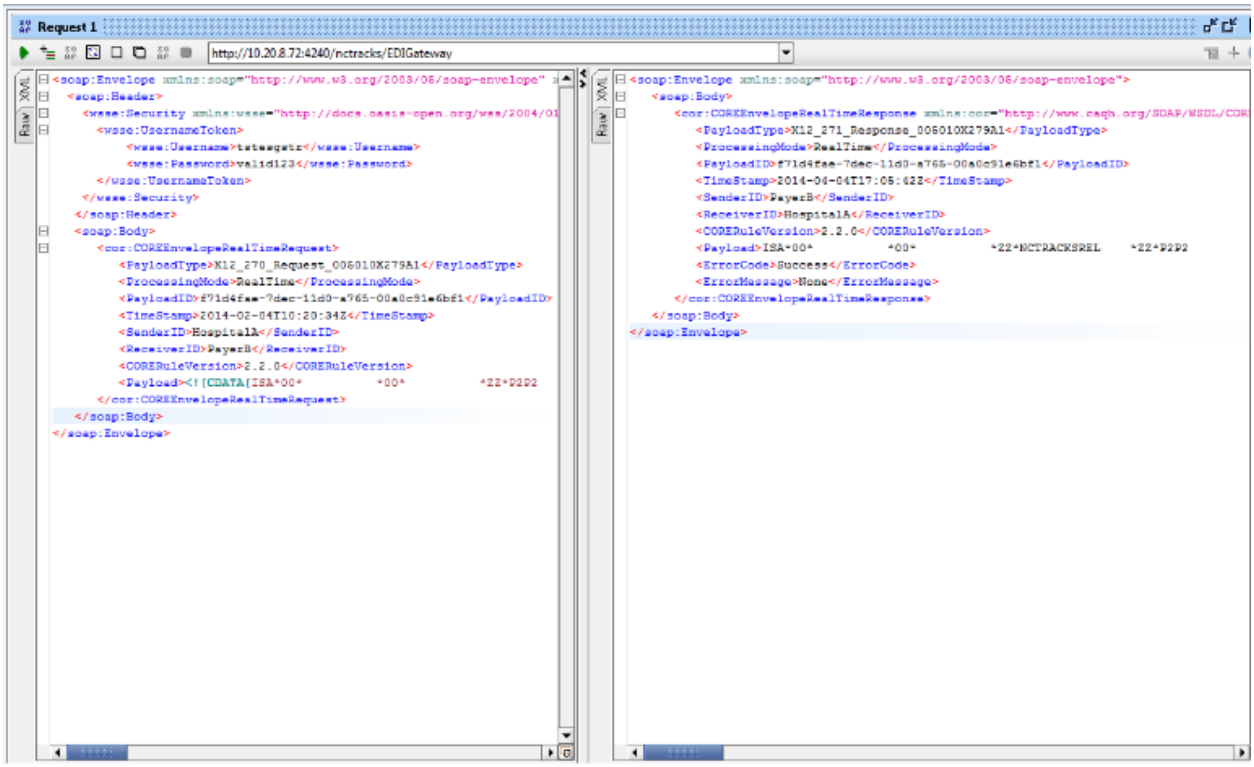
Example of the Response from a Batch Results Retrieval and Response:



Real-time Submission

- Users can submit real-time 270 or 276 single requests via SOAP.
- Only one transaction request within the X12 270 or 276 can be sent at a time. If more than one request is sent in the X12 file, an X12 271 or 277 response will be sent for the first request in the file and all other requests will be ignored.
- The X12 271 or 277 response is returned in the Payload of the SOAP response.

Example of a RealTime submission and response:



4.2.5.3 MIME for 270/271 and 276/277

NCTracks has the following submission types for MIME transmittal. The screenshots below are examples only. Sample 270, 271, and 999 Request SOAP and MIME clients are included in Appendices C, D, and E, respectively. A sample 999 Submission SOAP and MIME client is included in Appendix H.

Batch and Real-time Submission

- Users can submit a Batch or Real-time 270 or 276 MIME request.
- A Batch Results Retrieval Request is used to request a 271 or 277 response for a submitted 270 or 276.

Example of a 270 Submission:

```
Content-Type: multipart/form-data; boundary=XbcY

Request:
--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

tstesgstr
--XbCY
Content-Disposition: form-data; name="Password"

valid123
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"

ISA*00*          *00*          *ZZ*3UY7           *ZZ*NCTRACKSREL    *140112*1237*^*(
```

Example of a 270 Submission Response:

```
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="PayloadType"

X12_BatchReceiptConfirmation
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="ProcessingMode"

Batch
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="TimeStamp"

2014-02-02T04:29:03Z
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="SenderID"

PayerB
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="ErrorCode"

'Success'
--E60A3C98-134A-4042-9328-B78707B34591
Content-Disposition: form-data; name="ErrorMessage"

'None'
--E60A3C98-134A-4042-9328-B78707B34591--
c:\curl>
```

Batch Submission Acknowledgment Retrieval Request

Users can request the X12 999 Acknowledgment for a 270 or 276 submission.

Example of an Acknowledgment Retrieval Request:

```
Content-Type: multipart/form-data; boundary=XbcY

Request:
--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_999_Request_005010X231A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

tstesgstr
--XbCY
Content-Disposition: form-data; name="Password"

valid123
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
```

Example of a TA1 Acknowledgment Retrieval Response:

```
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="PayloadType"

X12_999_Response_005010X231A1
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="ProcessingMode"

Batch
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="PayloadLength"

154
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="TimeStamp"

2014-02-02T04:40:38Z
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="SenderID"

PayerB
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="CheckSum"

4472f1a9fb47a2ce12601dc7462fe6b4f9fe19bf
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="Payload"

ISA*00*          *00*          *ZZ*NCTRACKSREL    *ZZ*DIRECTCONNECT  *140131*
4*^*00501*140310934*0*P*:~TA1*147337265*131206*1539*R*008~IEA*0*140310934~
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="ErrorCode"

'Success'
--CEA9F38B-5027-D7EB-E37A-86B877FBE3EF
Content-Disposition: form-data; name="ErrorMessage"

'None'
```

Batch Results Retrieval Request

Users can request the 271 or 277 responses for a 270 or 276 request.

Example of a Batch Results Retrieval Request:

```
Content-Type: multipart/form-data; boundary=XbcY

Request:
--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_005010_Request_Batch_Results_271
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

tstesgstr
--XbCY
Content-Disposition: form-data; name="Password"

valid123
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
```

Example of a Batch Results Retrieval Response:

```
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="PayloadType"

X12_271_Response_005010X279A1
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="ProcessingMode"

Batch
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6ab9
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="PayloadLength"

16554
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="TimeStamp"

2014-02-13T15:57:16Z
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="SenderID"

PayerB
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="CheckSum"

ef0c5a2223edcf6830888fe5c077aa888546f32e
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="Payload"

ISA*00*          *00*          *ZZ*NCTRACKSBAT    *ZZ*SITTEST        *1402
GS*HB*NCMMISREL*SITTEST*20140213*105438*440000152*X*005010X279A1~ST*271*44
Content-Disposition: form-data; name="ErrorCode"

'Success'
--7DA6DDA5-86FF-24B9-0691-B221BD36F187
Content-Disposition: form-data; name="ErrorMessage"

'None'
--7DA6DDA5-86FF-24B9-0691-B221BD36F187--
```

Batch Results Acknowledgment Submission
Users can submit a RealTime 270 or 276 request.

Example of a RealTime request:

```
Content-Type: multipart/form-data; boundary=XbcY

Request:
--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

tstesgstr
--XbCY
Content-Disposition: form-data; name="Password"

valid123
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
```

4.2.6 CAQH-CORE Phase III Connectivity (835 and 820)

Overview

NCTracks supports CAQH-CORE Phase III compliant SOAP and MIME interfaces that allow Trading Partners to programmatically request batch 005010X221A1 835 Health Care Claim Payment Advice and 005010X218 820 Group Premium Payment For Insurance Products. Trading Partners are also allowed to programmatically submit a 005010X231A1 TA1/999 Implementation Acknowledgment for Health Care Insurance for batch 005010X221A1 835 Health Care Claim Payment Advice and 005010X218 820 Group Premium Payment For Insurance Products. Refer to Section 4.2.7, CAQH-CORE Phase II and III – Submitting 999 Transactions, to submit a batch 999 to NCTracks. Additional information about the Phase III interface can be found at http://www.caqh.org/CORE_phase3.php.

User Requirements

Users are required to be active Trading Partners and have a valid TSN and NCID. For Trading Partner enrollment information, refer to Section 2.2.1, Trading Partner/Providers Enrollment. The Trading Partner must also be provisioned to submit using the CAQH-CORE Phase III methodology. For user provisioning for CAQH-CORE, refer to Section 2.2.2.3, User Role Setup Instructions.

Software Requirements

NCTracks does not provide software for SOAP or MIME connectivity. Trading Partners must obtain their own software for submittal. NCTracks requires version 2.2.0 for SOAP and MIME clients. Most programming languages support SOAP and MIME clients and contain documentation to help Trading Partners create a client that can send/receive information to this interface. Sample 835 and 820 SOAP and MIME clients are included in Appendices F and G, respectively. A sample 999 Submission SOAP and MIME client is included in Appendix H. The samples of SOAP and MIME are only examples, and are not intended to function as-is.

The Trading Partner will need to understand how to write the program and handle the response appropriately. Follow the CORE Phase III specifications described above, which contain detailed instructions about the format of the request and the response.

For more information pertaining to CORE Phase III requirements and SOAP and MIME submissions, please refer to the following websites:

- CORE Phase III: http://www.caqh.org/CORE_phase3.php
- SOAP: http://www.w3.org/TR/soap/
- MIME Multipart: http://www.w3.org/Protocols/rfc1341/7_2_Multipart.html

CAQH-CORE Production

NCTracks will not provide ongoing testing for SOAP and MIME connectivity. Refer to Section 4.2.6.1, SOAP and MIME Attributes for 835 and 820 for production file setup instructions.

Production files should be submitted to the following URL:

https://edi.nctracks.nc.gov/EDIGateway

NCTracks Requirements for Requesting an 835 and 820 SOAP or MIME File
Trading Partners may only request an 835 or 820 file, via a SOAP or MIME request, that was created within the last 90 days. If the trading partner needs an 835 or 820 file that was created greater than 90 days ago, they must contact EDI Technical Assistance (refer to Section 2.1, Working Together, for contact information). The Trading Partner must have the Payment Date, TSN, and NPI/Atypical ID to request an 835 or 820 file.

CORE Interface Parameters
The CORE interface requires submission of certain parameters. The following sections describe specific information for SOAP and MIME submissions and the expectations of NCTracks.

4.2.6.1 SOAP and MIME Attributes for 835 and 820

Payload Type
The Trading Partner must submit one of the following Payload types:

- X12_835_Request_005010X221A1
  - This PayloadType requests the X12 835 file.
  - The Payment Date, TSN, and NPI/Atypical ID are required to receive the X12 835 file.
  - The Trading Partner will receive an X12_835_Response_005010X221A1. The response may have the following three (3) types of messages:
    - The Trading Partner will receive a response with the X12 835 as an attachment.
    - The Trading Partner will receive the message “No Files Found Specific to Corresponding Input”.
    - The Trading Partner will receive an appropriate error message based on the error created. Refer to Section 4.2.8, SOAP and MIME Error Messages for possible error messages.
- X12_820_Request_005010X218A1
  - This PayloadType requests the X12 820 file.
  - The Payment Date, TSN, and NPI/Atypical ID are required to receive the X12 820 file.
  - The Trading Partner will receive an X12_005010_Response_005010X218A1. The response may have the following three (3) types of messages:
    - The Trading Partner will receive a response with the X12 820 as an attachment.
    - The Trading Partner will receive the message “No Files Found Specific to Corresponding Input”.
    - The Trading Partner will receive an appropriate error message based on the error created. Refer to Section 4.2.8, SOAP and MIME Error Messages for possible error messages.

ProcessingMode
The ProcessingMode is always Batch for 835 and 820 transactions.

PayloadID
The PayloadID is used to link request and response files. A unique ID specific to an NCID should be used that will help identify the response to the request, and the PayloadID should not be duplicated (see the naming standards in the Payload description below). Note that only one PayloadID per message can be used. The PayloadID should be in the ISO UUID format. Please refer to the XSD and WSDL version 2.2.0, located on the CAQH-CORE website at http://www.caqh.org/SOAP/WSDL/.

PayloadLength
PayloadLength is for Batch submissions only and should be determined by the Trading Partner.

TimeStamp
The format of the TimeStamp must follow the conventions found at http://www.w3.org/TR/xmlschema11-2/#dateTime.

An example of a valid TimeStamp is 2014-02-01T10:30:55-00:00.

SenderID
The SenderID should identify the sender. It can be up to 50 alphanumeric characters and cannot contain spaces.

ReceiverID
Must contain “NCTracks”.

CORERuleVersion
Must contain “2.2.0”.

CheckSum
NCTracks requires the SHA-1 digest for the Payload only calculation for the CheckSum. For CheckSum naming standards, please refer to the XSD and WSDL, version 2.2.0, located on the CAQH-CORE website at http://www.caqh.org/SOAP/WSDL/.

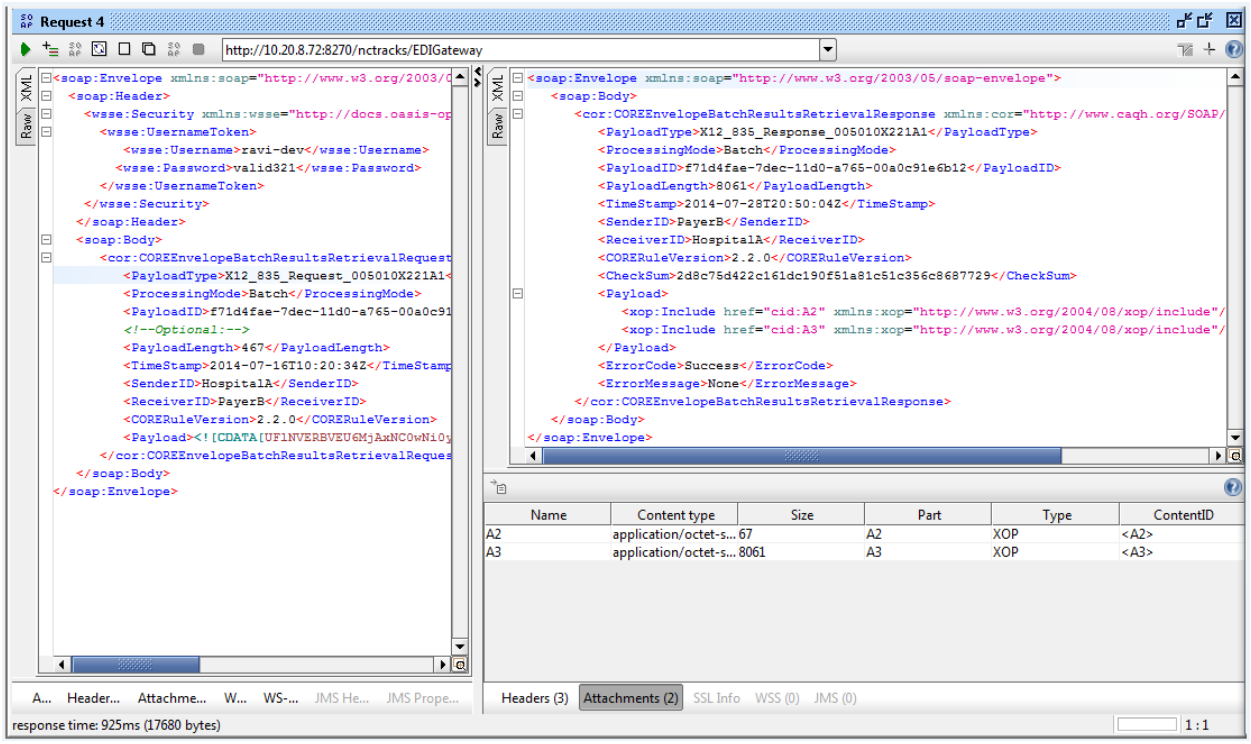
Payload
The Payload of 835/820 should be in base64 format and contains the following three variables:
{<PYMTDATE:ccyy-mm-dd>,<PID:integer(exact 8 or 10 digits)>,<TSN:alphaNumeric(4)>}

The base64 value of PYMTDATE:2014-06-24,PID:50264046, TSN:SRHI would be:
lNVERBVEU6MjAxNC0wNi0yNCxQSUQ6NTAyNjQwNDYsVFNOOlNSSEk=

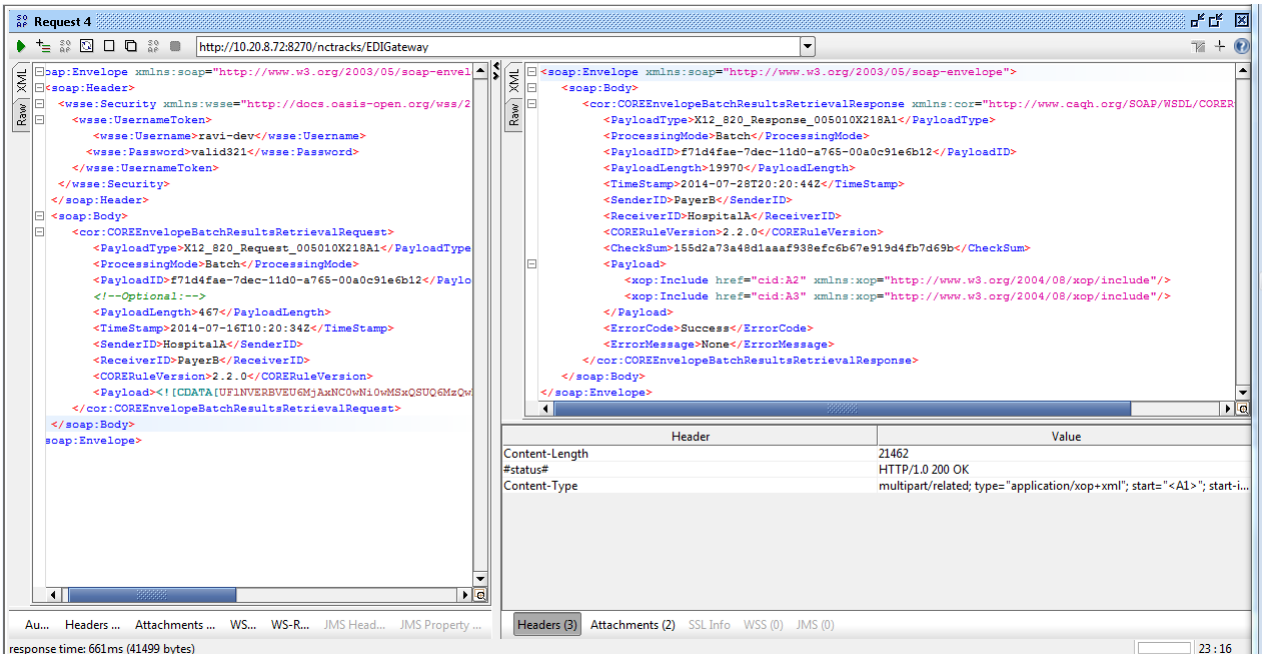
4.2.6.2 SOAP for 835 and 820

NCTracks has the following submission types for SOAP transmittal. The following screenshots are examples only. The actual attributes for a SOAP submission are listed in Section 4.2.6.1, SOAP and MIME Attributes for 835 and 820. Sample 835 and 820 SOAP and MIME clients are included in Appendices F and G, respectively. A sample 999 Submission SOAP and MIME client is included in Appendix H.

Example of Batch SOAP 835 Request to receive the X12 file and the response:



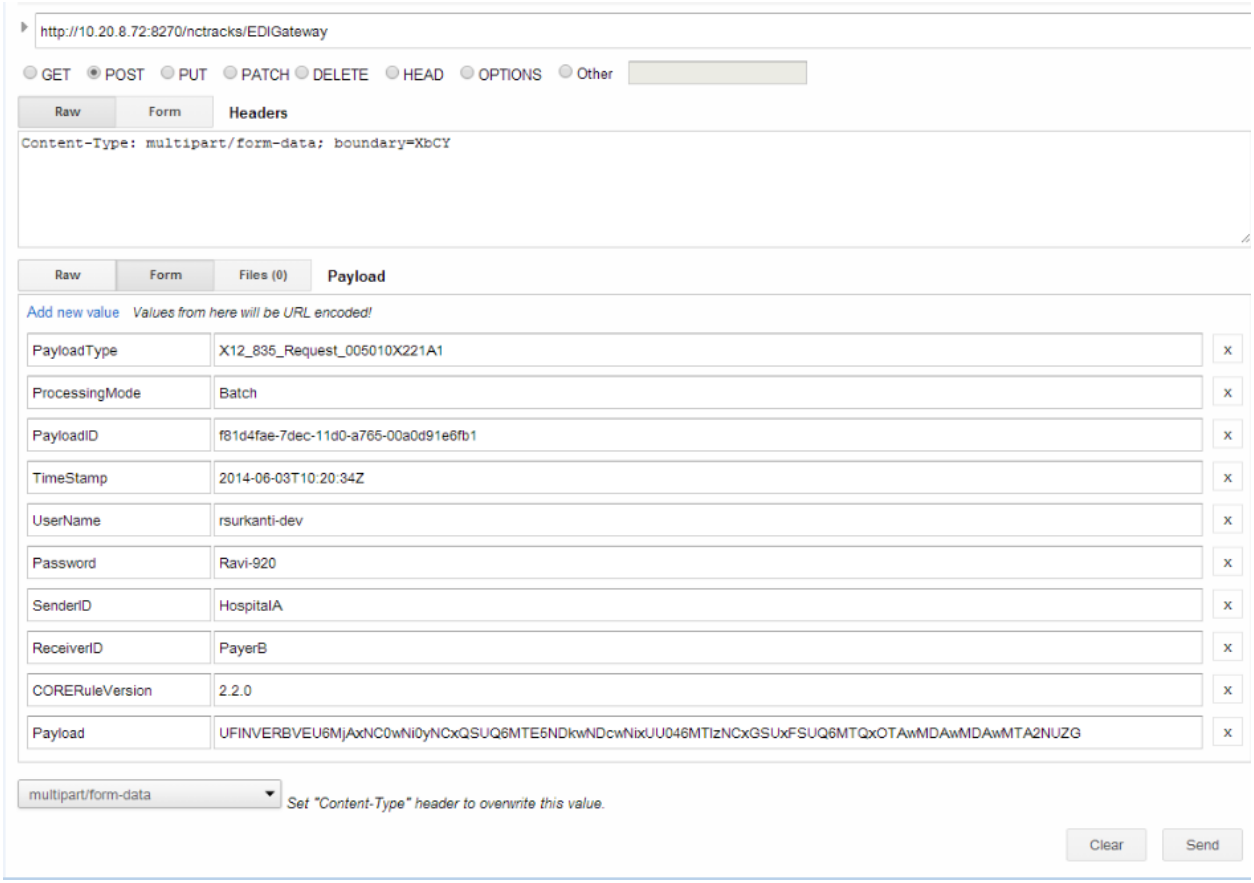
Example of Batch SOAP 820 Request to receive the X12 file and the response:



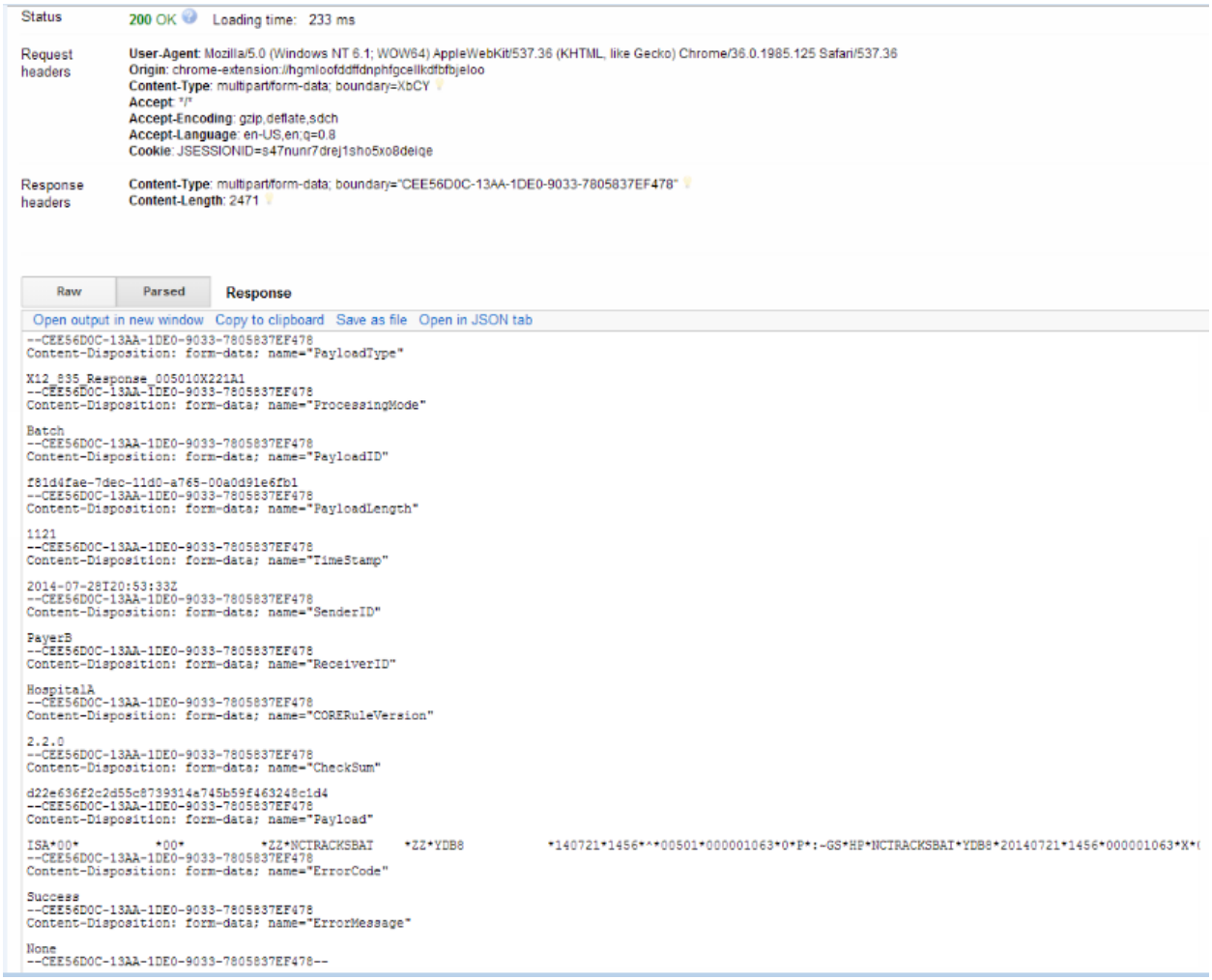
4.2.6.3 MIME for 835 and 820

NCTracks has the following submission types for MIME transmittal. The following screenshots are examples only. The actual attributes for a MIME submission are listed in Section 4.2.6.1, SOAP and MIME Attributes for 835 and 820. Sample 835 and 820 SOAP and MIME clients are included in Appendix F and Appendix G, respectively. A sample 999 Submission SOAP and MIME client is included in Appendix H.

Example of Batch MIME 835 Request to receive the X12 file:



Example of Batch MIME 835 Response to the Request to receive the X12 file:



Status 200 OK Loading time: 233 ms

Request headers
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Origin: chrome-extension://hgmloofddffdnphfgcellkdfbfbjeloo
Content-Type: multipart/form-data; boundary=XbCY
Accept: */*
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=s47nunr7drej1sho5xo8deiqe

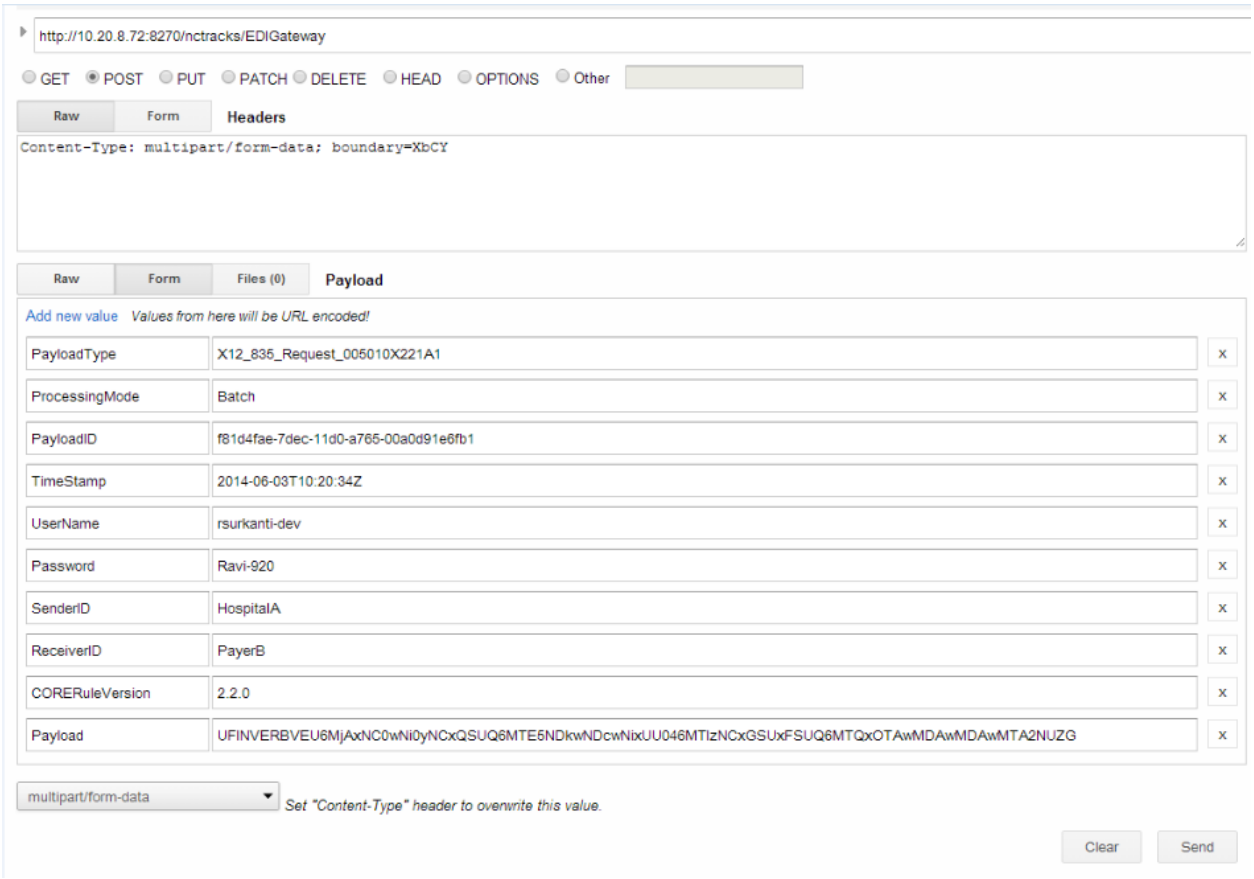
Response headers
Content-Type: multipart/form-data; boundary="CEE56D0C-13AA-1DE0-9033-7805837EF478"
Content-Length: 2471

Raw Parsed **Response**

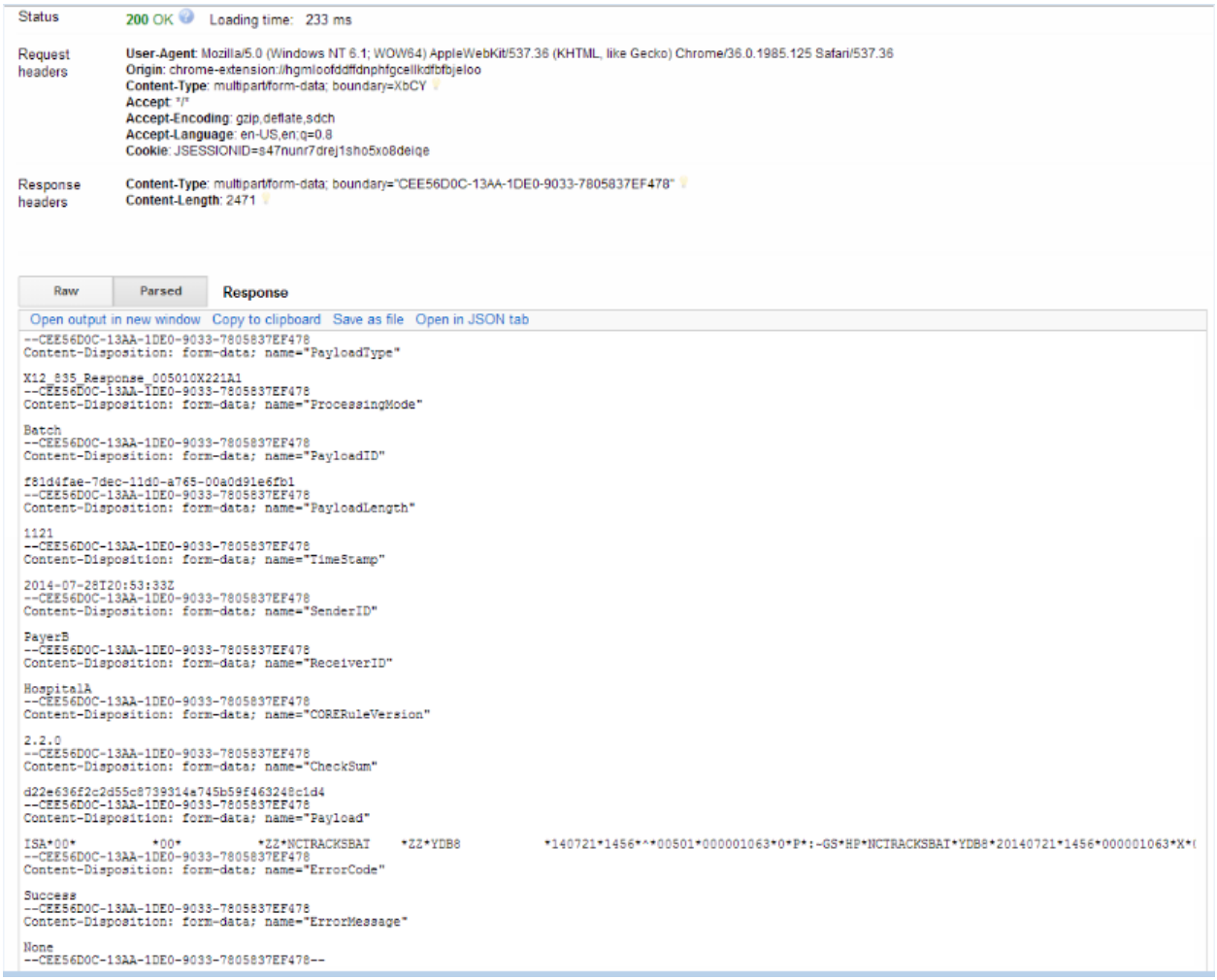
Open output in new window Copy to clipboard Save as file Open in JSON tab

```
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="PayloadType"

X12_835_Response_005010X221A1
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="ProcessingMode"

Batch
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="PayloadLength"

1121
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="TimeStamp"

2014-07-28T20:53:33Z
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="SenderID"

PayerB
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="CheckSum"

d22e636f2c2d55c8739314a745b59f463248c1d4
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="Payload"

ISA*00*          *00*          *ZZ*NCTRACKSBAI    *ZZ*YDB8           *140721*1456*^*00501*000001063*0*P*:~GS*HP*NCTRACKSBAI*YDB8*20140721*1456*000001063*X*(
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="ErrorCode"

Success
--CEE56D0C-13AA-1DE0-9033-7805837EF478
Content-Disposition: form-data; name="ErrorMessage"

None
--CEE56D0C-13AA-1DE0-9033-7805837EF478--
```

Example of Batch MIME 820 Request to receive the X12 file:



Example of Batch MIME 820 Response to the Request to receive the X12 file:



4.2.7 CAQH-CORE Phase II and III – Submitting 999 Transactions

Users can submit a 999 or TA1 Acknowledgment for the Batch 271, 277, 820, and 835 files received from NCTracks via SOAP or MIME submission methodologies.

4.2.7.1 SOAP and MIME Attributes for 999 Submission

PayloadType

The Trading Partner must submit one of the following Payload types:

- X12_999_SubmissionRequest_005010X231A1 (used to submit a 999 to NCTracks)
- X12_TA1_SubmissionRequest_005010X231A1 (used to submit a TA1 to NCTracks)

ProcessingMode

The Trading Partner must submit Batch 999 or TA1 only.

PayloadID

The PayloadID is used to link request and response files. A unique ID specific to an NCID should be used that will help identify the response to the request, and the PayloadID should not be duplicated (see the naming standards in the Payload description below). Note that only one

PayloadID per message can be used. The PayloadID should be in the ISO UUID format. Please refer to the XSD and WSDL version 2.2.0, located on the CAQH-CORE website at http://www.caqh.org/SOAP/WSDL/.

PayloadLength
PayloadLength is for Batch submissions only and should be determined by the Trading Partner.

TimeStamp
The format of the TimeStamp must follow the conventions found at http://www.w3.org/TR/xmlschema11-2/#dateTime.

An example of a valid TimeStamp is 2014-02-01T10:30:55-00:00.

SenderID
The SenderID should identify the sender. It can be up to 50 alphanumeric characters and cannot contain spaces.

ReceiverID
Must contain “NCTracks”.

CORERuleVersion
Must contain “2.2.0”.

CheckSum
NCTracks requires the SHA-1 digest for the Payload only calculation for the CheckSum. For CheckSum naming standards, please refer to the XSD and WSDL, version 2.2.0, located on the CAQH-CORE website at http://www.caqh.org/SOAP/WSDL/.

Payload
For RealTime submissions, the Payload contains the ASC X12 data for the submission. The ASC X12 file must be valid with the correct settings in the envelope. Refer to the appropriate Companion Guide for the submission for the correct settings and NCTracks rules, located at https://www.nctracks.nc.gov/content/public/providers/provider-trading-partners.html.

For Batch submissions, the Payload contains the name of the ASC X12 batch file, and the file should be submitted as an attachment. The ASC X12 file must be valid with the correct settings in the envelope. Refer to the appropriate Companion Guide for the submission for the correct settings and NCTracks rules, located at https://www.nctracks.nc.gov/content/public/providers/provider-trading-partners.html.

The ASC X12 file must adhere to the following naming standards.

Naming Standards for X12 Inbound Transactions

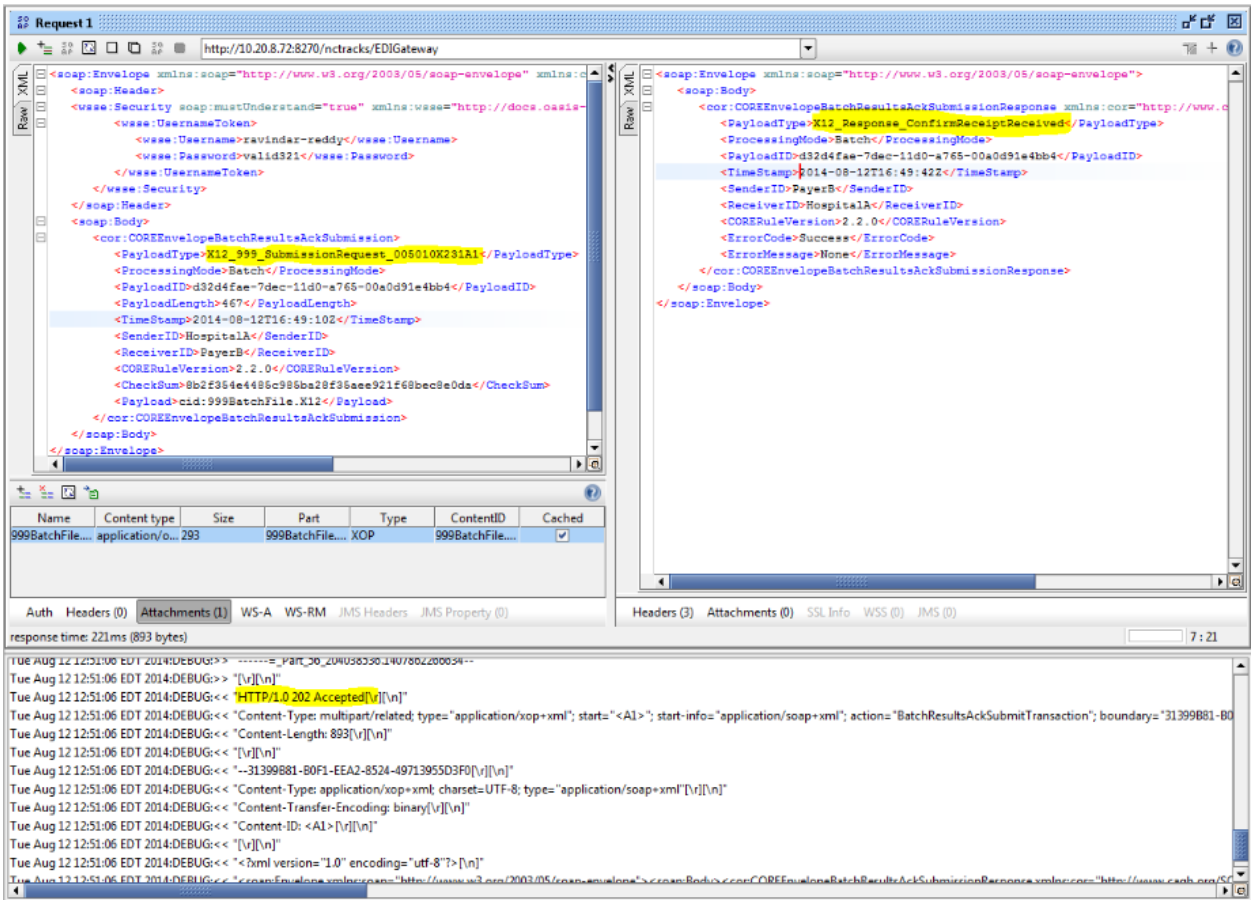
- File extensions not accepted:

  *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd, *.pif, *.pot, *.reg, *.scr, *.sct, *.shb, *.shs, *.sys, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh, *.zip
- Special characters (for example, hyphen, asterisk, question mark) are not allowed in file names.
- Zip files are not allowed for SOAP transmittals.

4.2.7.2 SOAP for 999 Submission

NCTracks has the following submission types for SOAP transmittal. The following screenshots are examples only. The actual attributes for a SOAP submission are listed in Section 4.2.7.1, SOAP and MIME Attributes for 999 Submission. A sample 999 Submission SOAP and MIME client is included in Appendix H.

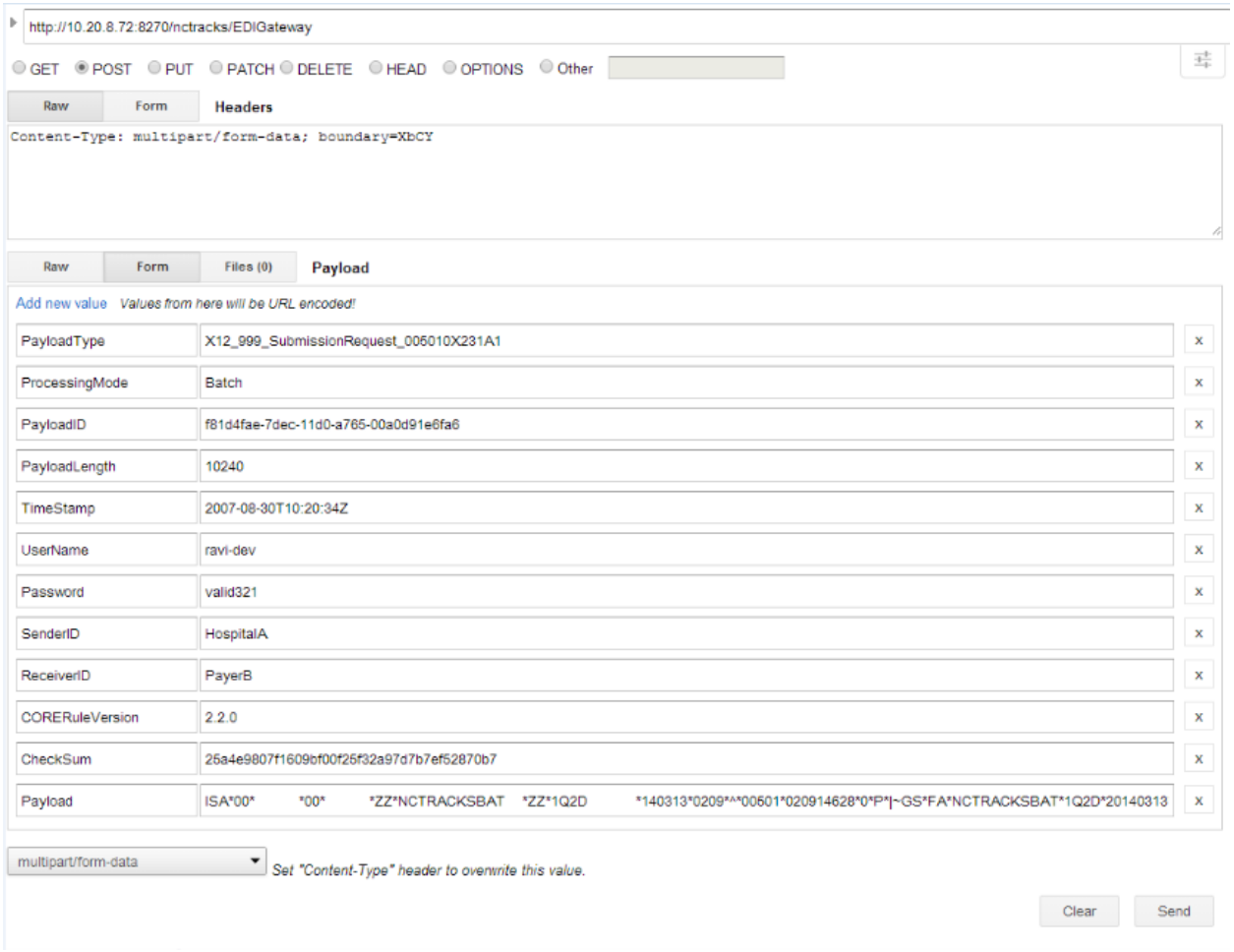
Example of a Batch Results Acknowledgment Submission Request and Response:



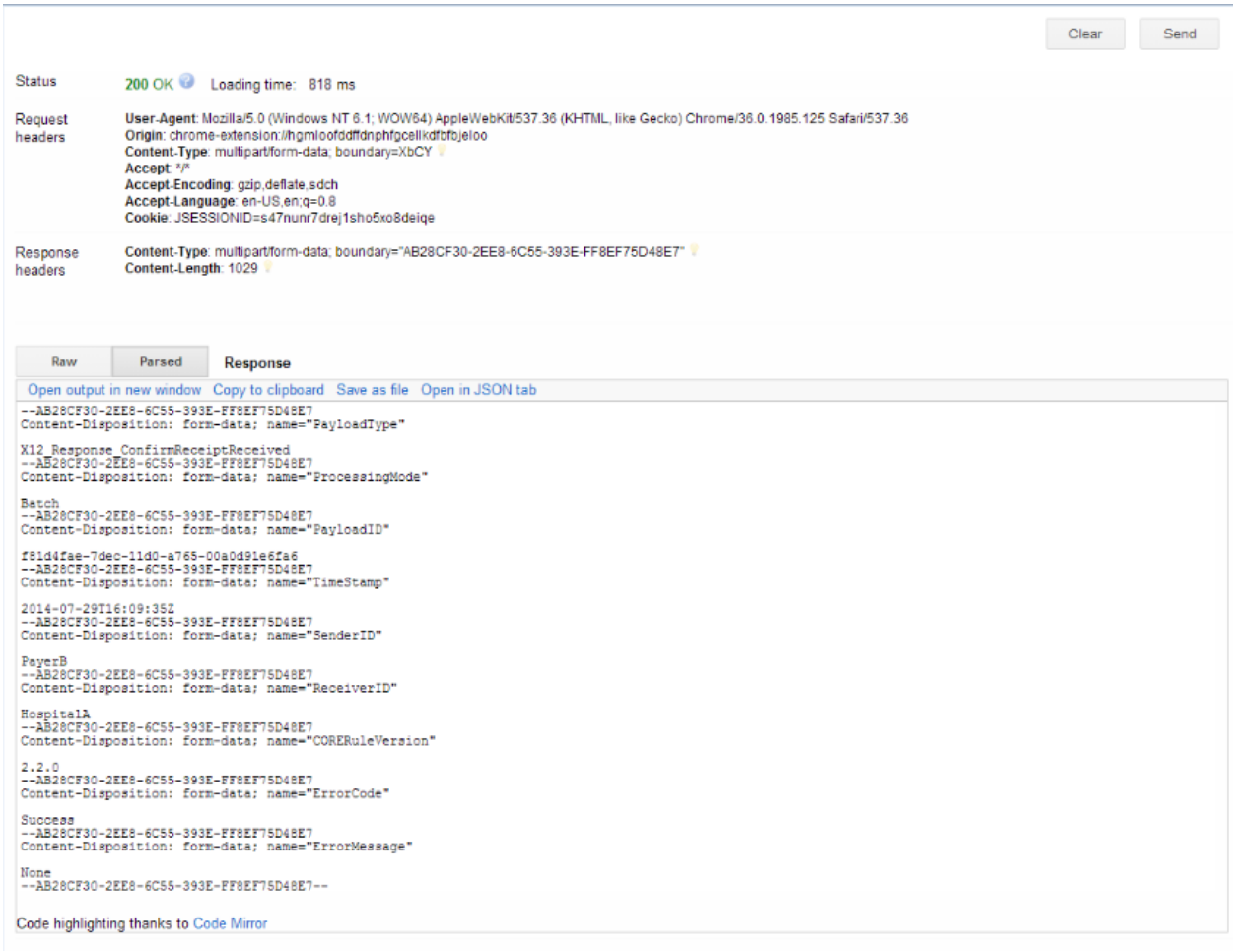
4.2.7.3 MIME for 999 Submission

NCTracks has the following submission types for MIME transmittal. The following screenshots are examples only. The actual attributes for a MIME submission are listed in Section 4.2.7.1, SOAP and MIME Attributes for 999 Submission. A sample 999 Submission SOAP and MIME client is included in Appendix H.

Example of a 999 Batch Results Acknowledgment:



Example of a 999 Batch Results Acknowledgment response:



4.2.8 SOAP and MIME Error Messages

Username and Password

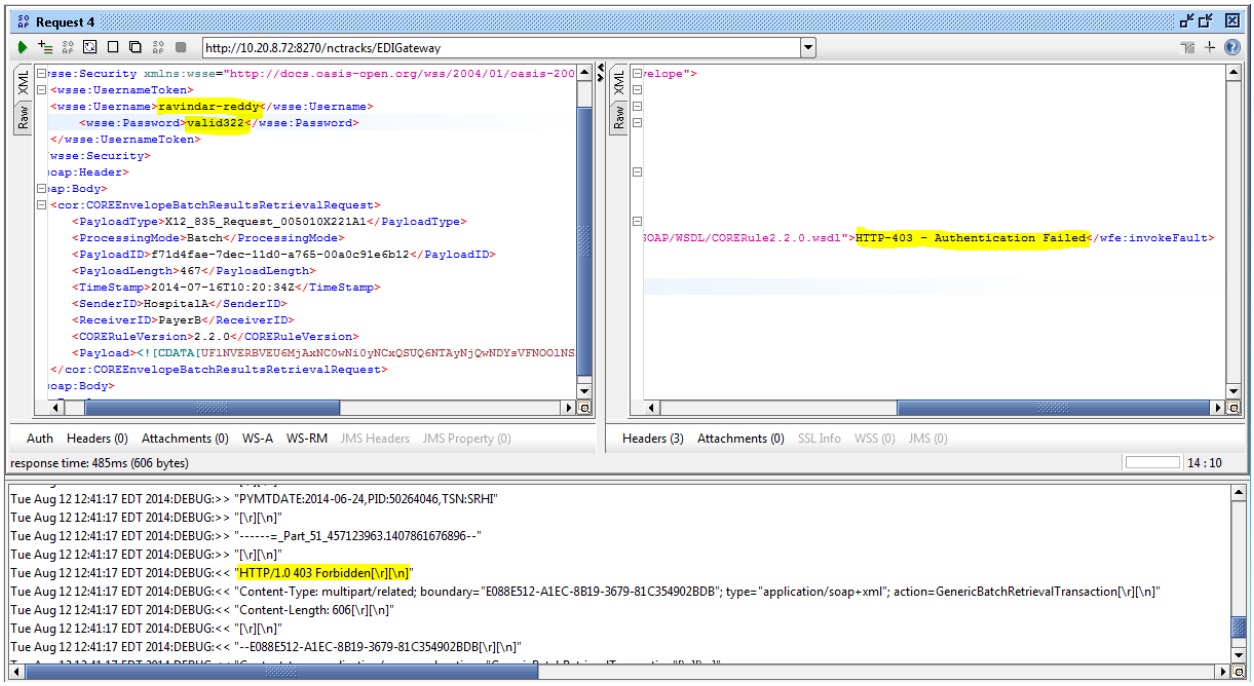
Trading Partners will use their respective NCID and Password for SOAP and MIME submissions. The NCID must be provisioned in NCTracks before any real-time or batch transactions can be submitted. The user will receive an error response if a submission attempt is made with an invalid NCID and Password. For user provisioning for CAQH-CORE, refer to Section 2.2.2.3, User Role Setup Instructions. The following table provides a summary of the error messages that can be received.

Error Code	Error Type	Error Description	Error Message Returned in SOAP/MIME
HTTP-403	Authentication Error	Invalid Username and Password	HTTP-403 – Authentication Failed
HTTP-403	Authentication Error	A valid NCID and Password, but not authorized to submit	AuthenticateAuthorizeService – Authentication Passed but Authorization failed
HTTP-403	Authentication Error	TSN not Active	AuthenticateAuthorizeService – Authentication Passed but Authorization failed

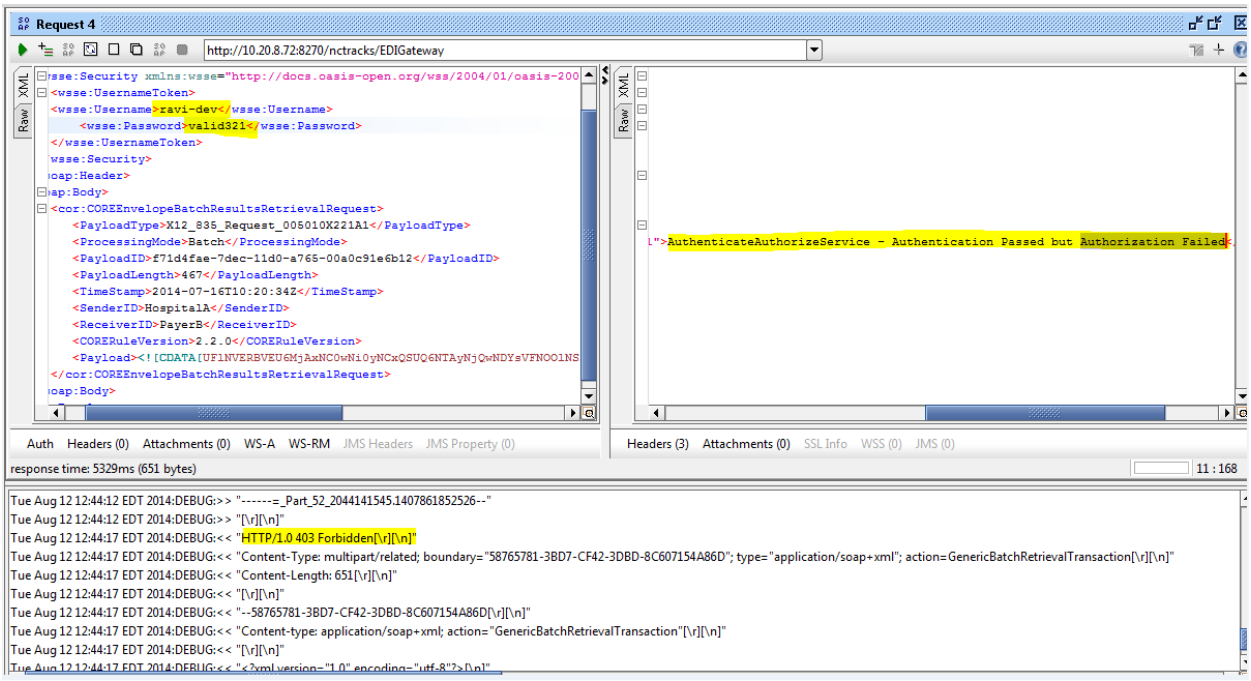
Error Code	Error Type	Error Description	Error Message Returned in SOAP/MIME
HTTP-403	Authentication Error	TSN not affiliated with NPI	AuthenticateAuthorizeService – Authentication Passed but Authorization failed
HTTP-400	Bad Request	Invalid TSN	Invalid TSN (Should be 4 Chars) <<Payload from request>>
HTTP-400	Bad Request	Invalid NPI or Atypical ID	Invalid PID (Length of the PID should be less than or equal to 10 Chars) <<Payload from request>>
HTTP-400	Bad Request	Invalid PayloadType	SchemaValidationScope-Error Occurred during Schema Validation
HTTP-400	Bad Request	Invalid PaymentDate	Invalid Payment Date (Should be less than or equal to 90 days from the Current Date) <<Payload from request>>
HTTP-200	Bad Request	No file found	Receiver – No Files Found Specific to Corresponding Input
HTTP-400	Bad Request	Payment Date outside the date range allowed	Invalid Payment Date (Should be less than or equal to 90 days from the Current Date) <<Payload from request>>

4.2.8.1 SOAP Error Message Examples

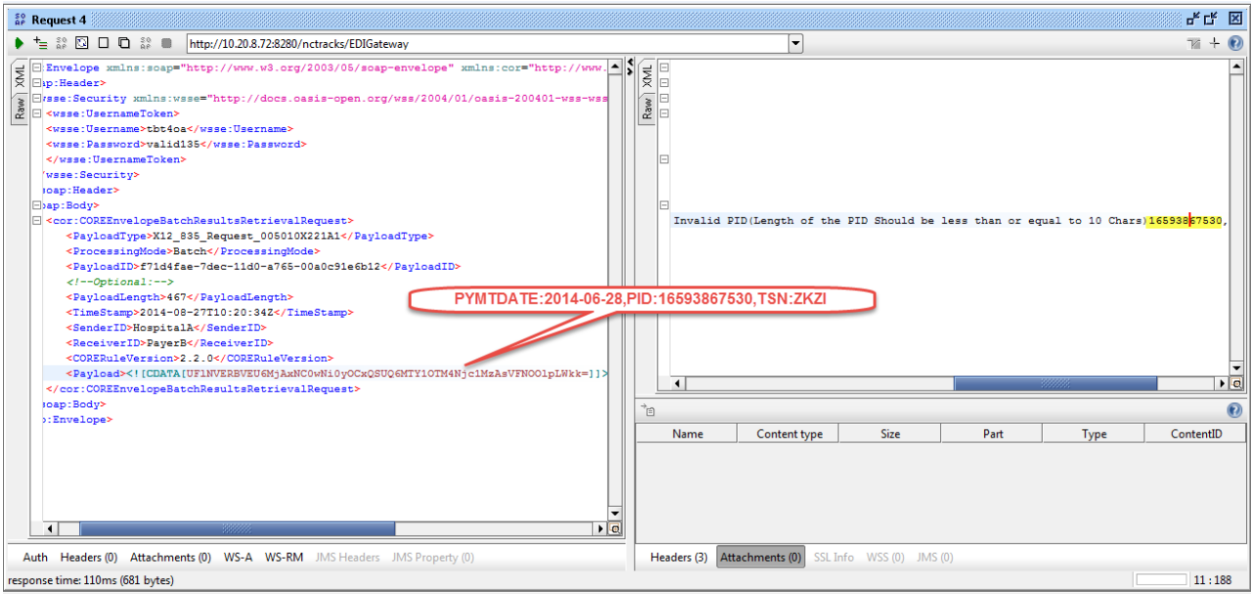
Example of an invalid Username and Password message:



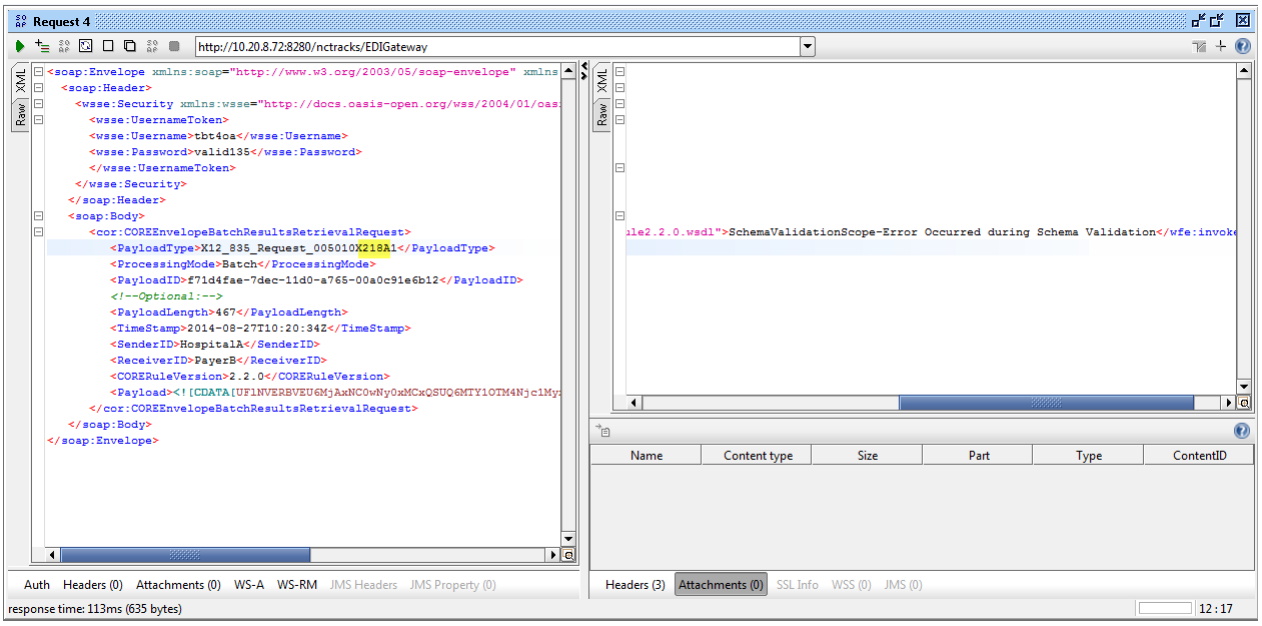
Example of a User with a valid NCID and Password, but not authorized to submit:



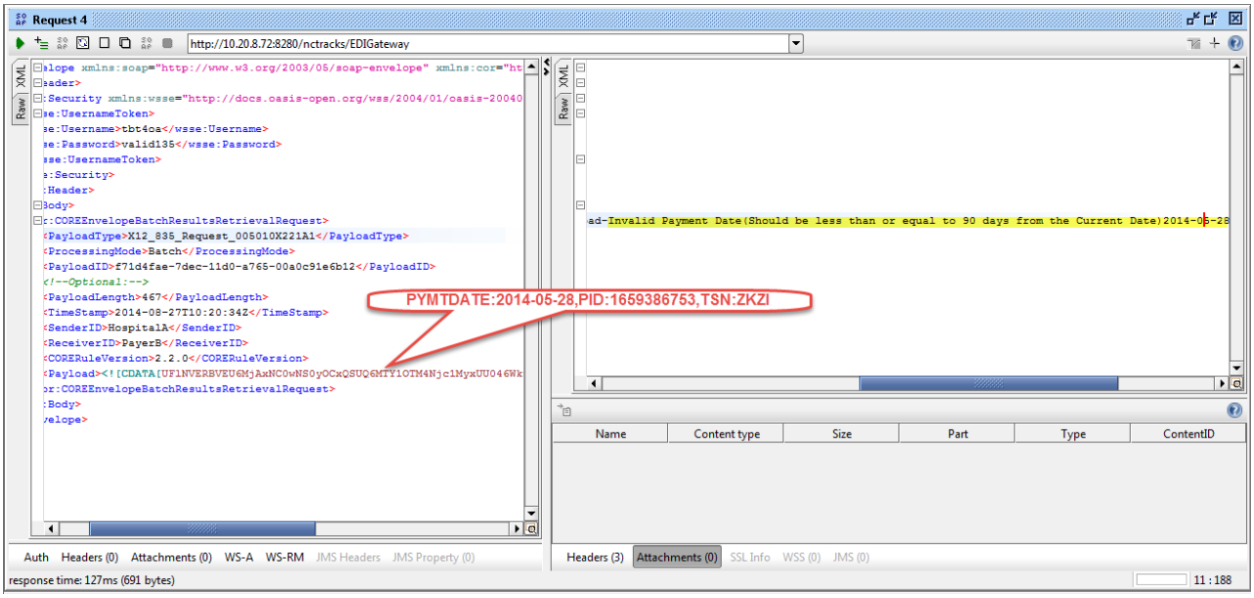
Examples of an invalid NPI or Atypical ID:



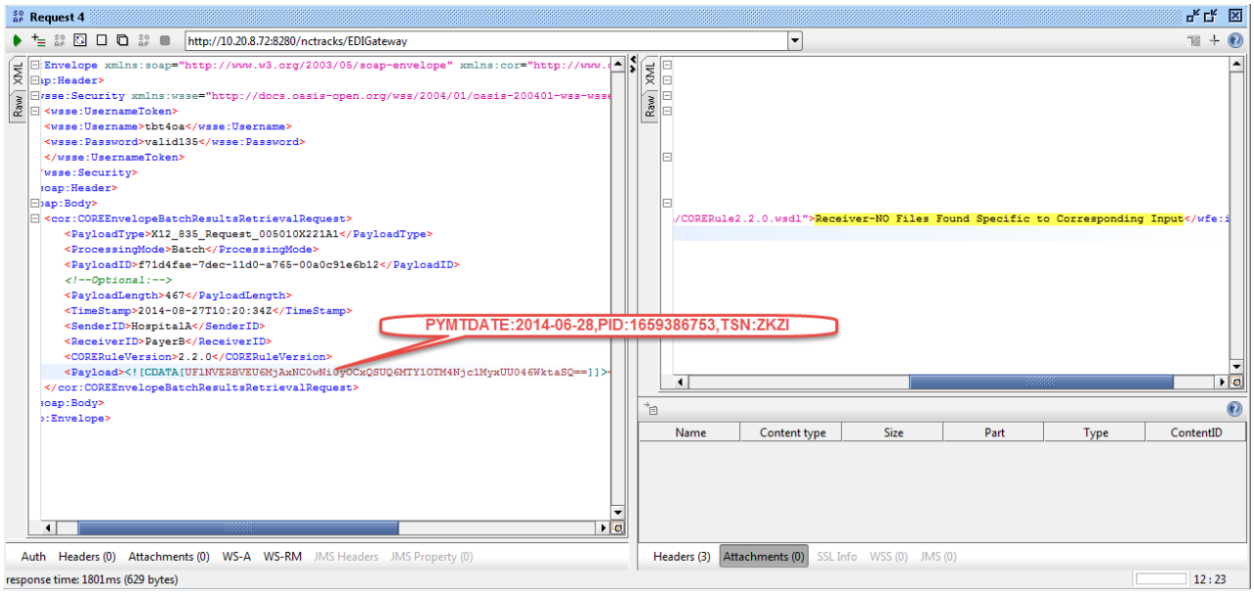
Example of an invalid PayloadType:



Example of an invalid PaymentDate:

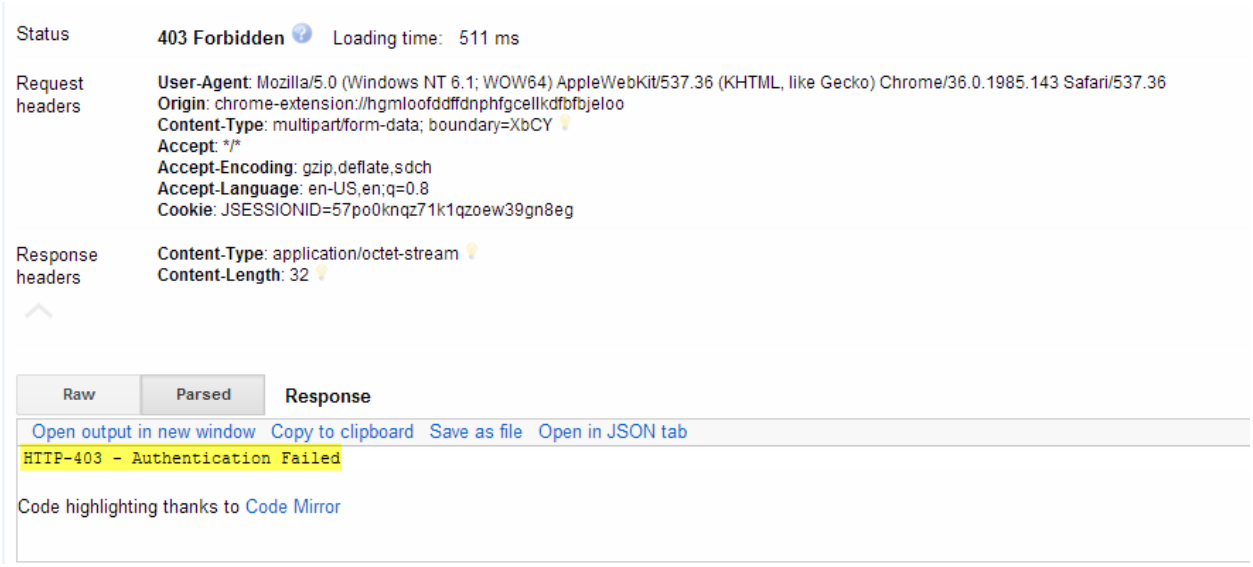


Example of no file found:



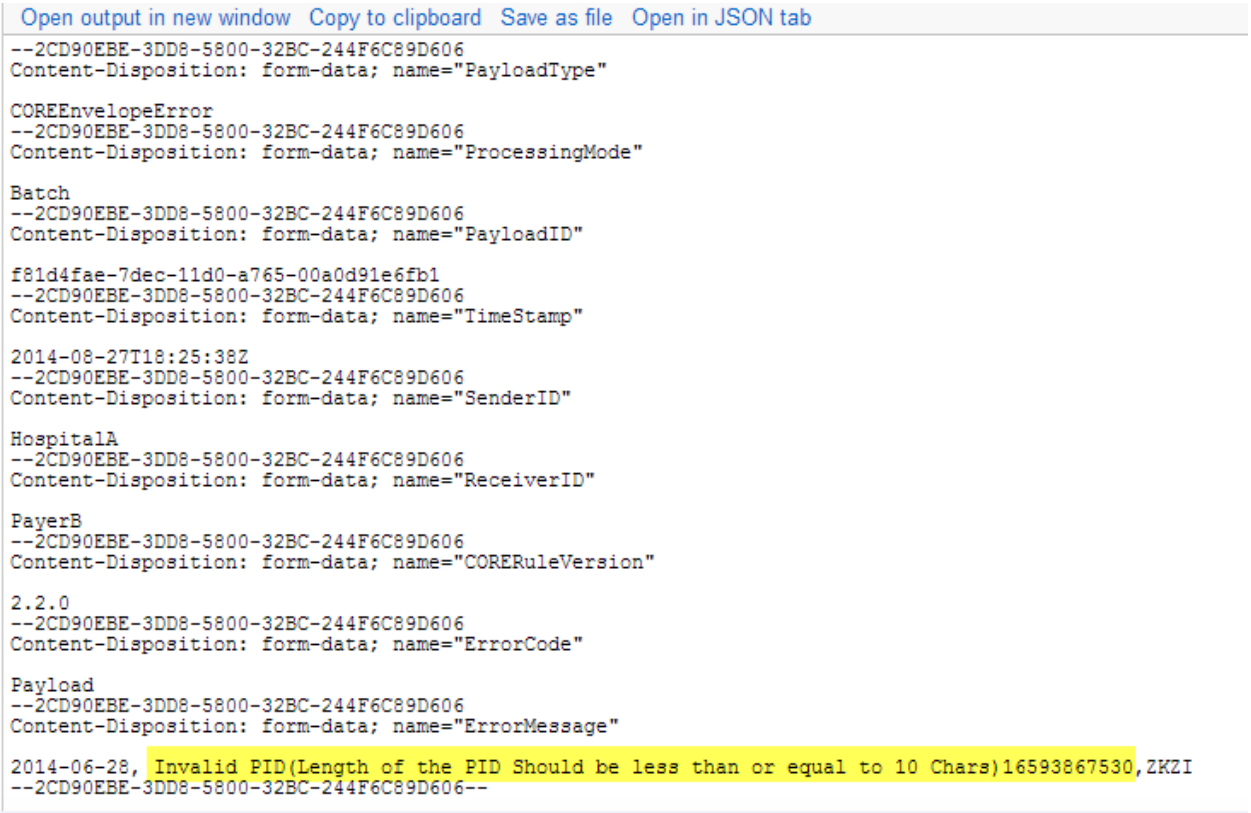
4.2.8.2 MIME Error Message Examples

Example of invalid Username and Password message:



Example of a User with a valid NCID and Password, but not authorized to submit:

Example of an invalid NPI or Atypical ID:



Example of an invalid PayloadType:

Raw | Parsed **Response**

Open output in new window | Copy to clipboard | Save as file | Open in JSON tab

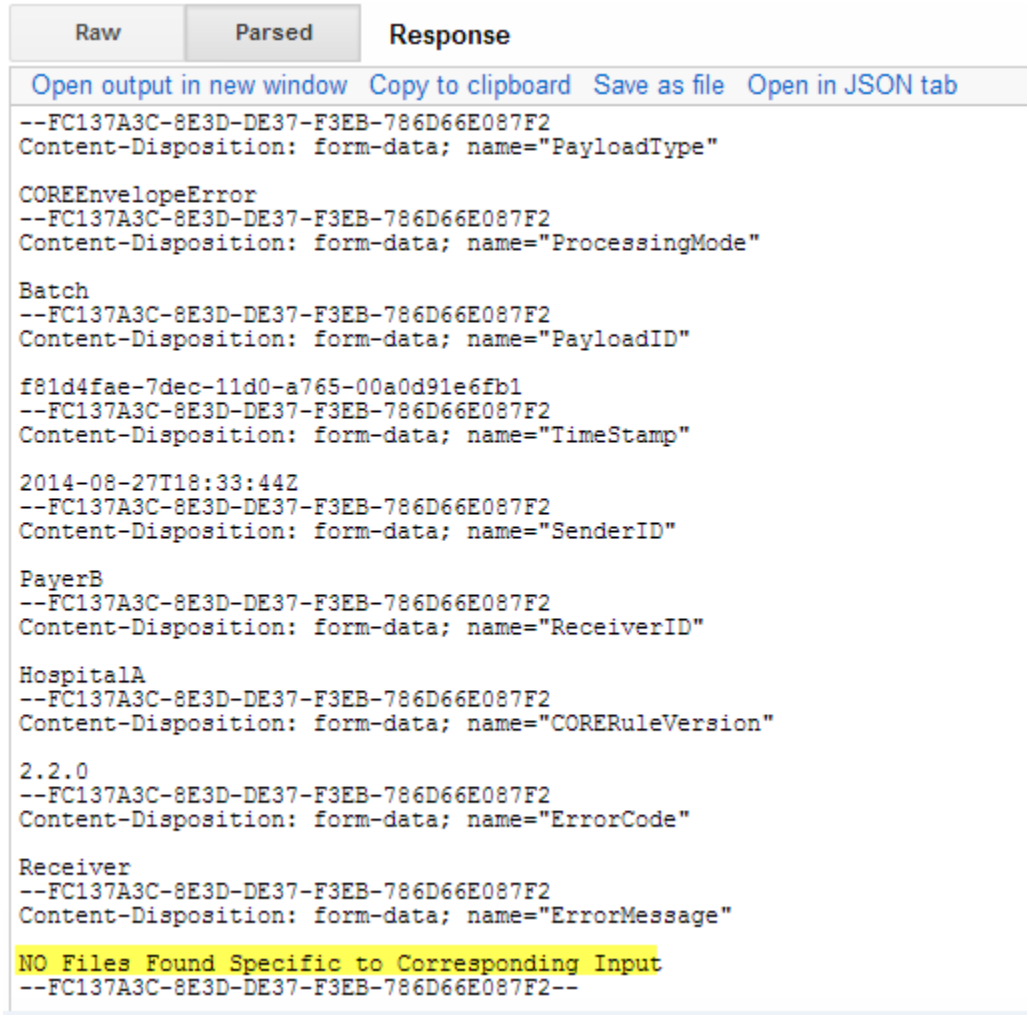
```
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="PayloadType"

COREEnvelopeError
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="ProcessingMode"

Batch
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="TimeStamp"

2014-08-28T14:06:20Z
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="SenderID"

PayerB
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="ReceiverID"

HospitalA
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="ErrorCode"

Sender
--5892FA07-7837-56B6-0BA7-0DF798D2972E
Content-Disposition: form-data; name="ErrorMessage"

[Error]instance file line:-1: cvc-elt.1:The element 'error' is wrong
No corresponding declaration is found in schema

--5892FA07-7837-56B6-0BA7-0DF798D2972E--
```

Example of an invalid PaymentDate:

Open output in new window Copy to clipboard Save as file Open in JSON tab

```
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="PayloadType"

COREEnvelopeError
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="ProcessingMode"

Batch
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="TimeStamp"

2014-08-27T18:20:12Z
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="SenderID"

HospitalA
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="ReceiverID"

PayerB
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="ErrorCode"

Payload
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD
Content-Disposition: form-data; name="ErrorMessage"

Invalid Payment Date(Should be less than or equal to 90 days from the Current Date)2014-05-28,1659386753,ZKZI
--3A61706D-68E0-F2CB-2396-33EB1B98ECAD--
```

Example of no file found:



5. Contact Information

5.1 EDI TECHNICAL ASSISTANCE

Phone: 1-800-688-6696, option #1

Email: NCMMIS_EDI_SUPPORT@gdit.com

Website: http://www.nctracks.nc.gov/provider/index.html

Companion Guides: http://www.nctracks.nc.gov/provider/guides/index.html

5.2 PROVIDER/TRADING PARTNER ENROLLMENT

Currently Enrolled Provider (CEP), Billing Agent Enrollment
Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

Website: https://www.nctracks.nc.gov/provider/providerEnrollment/

NCTracks Enrollment
Phone: 1-800-688-6696

Email: NCTracksprovider@nctracks.com

Website: https://www.nctracks.nc.gov/content/public/providers/provider-enrollment.html

5.3 CONNECTIVITY AND OTHER TECHNICAL ISSUES

Phone: 1-800-688-6696, option #1

5.4 WEB PORTAL ISSUES

Phone: 1-800-688-6696, option #2

5.5 SECURITY AND PRIVACY ISSUES

Phone: 1-800-688-6696, option #1
(Please inform the help desk that you have a question or concern relating to privacy or security.)

Email: ncmmissecurity@gdit.com

6. Control Segments / Envelopes

The TSN referenced in the following tables is provided by NCTracks after the Trading Partner completes the Trading Partner Agreement (TPA).

6.1 ISA-IEA

Sender and Receiver Codes

Transaction	ISA06 (Interchange Sender ID)	ISA08 (Interchange Receiver ID)
270 batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
270 interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
276 batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
276 interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
834 batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837D batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837D interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
837I batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837I interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
837P batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837P interactive	Transaction Supplier Number (TSN)	NCTRACKSREL

6.2 GS-GE

Sender and Receiver Codes

Transaction	GS02 (Application Sender's Code)	GS03 (Application Receiver's Code)
270 batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
270 interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
276 batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
276 interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
834I batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837D batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837D interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
837I batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837I interactive	Transaction Supplier Number (TSN)	NCTRACKSREL
837P batch	Transaction Supplier Number (TSN)	NCTRACKSBAT
837P interactive	Transaction Supplier Number (TSN)	NCTRACKSREL

NCTracks supports sending multiple transaction types in the same ISA/IEA. Each transaction type must be within a separate GS level.

NCTracks does not support multiple ISA/IEA submissions in the same file. It will create a TA1 or F-File as described in Section 7, Acknowledgments and Reports.

NCTracks expects a segment terminator (~) at the end of each segment, as defined in Section B.1.1.2.5, Delimiters of all (837P, 837D, 837I, 270/271, 276/277, 834) TR3 documents.

In addition:

- NCTracks does not accept Carriage Return (CR), Line Feed (LF), or Carriage Return Line Feed (CRLF) characters as segment terminators.
- NCTracks will accept files with or without Carriage Return Line Feed (CRLF) characters, but if the CRLF character is sent, a segment terminator is still required.
- There should not be any spaces or any junk characters after the end of the IEA segment.

Files without a segment delimiter, with an unidentified segment terminator, or with spaces after the IEA segment will receive a negative TA1 and will not be processed.

6.3 ST-SE

NCTracks has no requirements for the contents of the ST and SE segments other than those specified in the Type 3 Technical Reports (X12 Implementation Guide) published by ASC X12N.

7. Acknowledgments and Reports

7.1 ASC X12 ACKNOWLEDGMENTS

7.1.1 Negative Interchange Acknowledgment (TA1) Negative File Transfer Status (F-File)

A file containing one of these responses will be returned only when a negative response is necessary because the file cannot be processed any further by the NCTracks translation engine. If this response is produced, a submitter will generally receive the response within 2 hours after the file is uploaded to NCTracks.

- Negative Interchange Acknowledgment (TA1) is returned only if the interchange control (ISA/IEA) structure validation fails **AND** if a TA1 was requested (inbound ISA14 = '1'). The TA1 may be returned only in response to a 5010 request.
- If a TA1 was not requested (inbound ISA14 ≠ '1') and the ASC X12 interchange control (ISA/IEA) structure fails validation, a text file is returned instead with the negative File Transfer Status (F-File). The F-File may be returned in response to ASC X12 5010.

Important Note: The TA1 Interchange Acknowledgment as implemented in NCTracks contains no values specific to NCTracks requirements or processing. Specifications for the TA1 Segment are published in the ASC X12C/005010X231 Implementation Guide Acknowledgment for Health Care Insurance (999).

7.1.2 Response Specific Information

The contents of the response file will vary based on the requested transaction type and may also contain one or more interchange controls (ISA/IEA) within a single file.

Implementation Acknowledgment (999) (5010 Only)

An Implementation Acknowledgment (999) transaction is returned to report the status of the Functional Group and each Transaction set it contains. It is generally available within 4 to 24 hours, unless the Interchange was rejected.

The 999 Implementation Guide Acknowledgments as implemented in NCTracks contain no values specific to NCTracks requirements or processing. Readers of this document are directed to the Type 3 Technical Report ASC X12C/005010X231 Implementation Acknowledgment for Health Care Insurance (999).

7.1.3 Preadjudication Editing

277 Health Care Information Status Notifications (Unsolicited) (U277)

In response to a 5010 real-time 837 Transaction Set, a 277 Health Care Information Status Notification (U277) Transaction Set is returned to report the status of each claim, generally within seconds, unless the Interchange or Functional Group was rejected.

Refer to the NCTracks Transaction Information Companion Guide for an overview of the NCTracks implementation of the ASC X12N/005010X212 277 Health Care Information Status Notification.

7.1.4 Acknowledgment Examples

7.1.4.1 Acknowledgments – Accepted

Accepted Transaction and Functional Group (5010 Only): 999 Implementation Acknowledgments

The 999 reports an accepted Functional Group. It contained one Transaction Set, an 837. The 999 is returned in response to all version 5010 transactions.

ISA*00* *00* *ZZ*NCTRACKSBAT *ZZ*348T *130522*1648*^*00501*164837519*0*P*|

GS*FA*NCTRACKSBAT*348T*20130522*1648*164837519*X*005010X231A1

ST*999*4001*005010X231A1

AK1*HC*1*005010X222A1

AK2*837*0001

IK5*A

AK9*A*1*1*1

SE*6*4001

GE*1*164837519

IEA*1*164837519

7.1.4.2 Acknowledgments – Rejected

1. Negative File Transfer Status: F-File

The F-File shows how rejected files are reported when rejection occurs at the first processing step.

Incomplete ISA segment

(W) Editing of USER1-090101083030-00-ISA-00-.x12 will not continue

*** FILE REJECTED ***

Other messages that can be sent within the “F-file” are:

*** FILE REJECTED: RECORD COUNT EXCEEDS CURRENT LIMITATIONS ***

*** FILE REJECTED: FILE SUBMISSION COUNT EXCEEDS CURRENT LIMITATIONS ***

2. TA1 Interchange Acknowledgment: Rejected Interchange

ISA*00* *00* *ZZ*NCTRACKSBAT *ZZ*5103 *130422*1350*^*00501*131120150*0*P*:

TA1*001530207*130214*1503*R*023

IEA*0*131120150

3. Rejected Transaction and Functional Group (5010 Only): 999 Implementation Acknowledgments

The 999 reports a rejected Transaction Set. Because there were no accepted Transaction Sets, the Functional Group is also rejected. The 999 is returned in response to all version 5010 transactions.

ISA*00* *00* *ZZ*NCTRACKSBAT *ZZ*8030 *130422*1403*^*00501*140343402*0*P*|

GS*FA*NCTRACKSBAT*8030*20130422*1403*140343402*X*005010X231A1

ST*999*140343402*005010X231A1

AK1*HC*1824*005010X222A1

AK2*837*1824

IK3*REF*11*2010*8

IK4*2*127*6*561102056

IK5*R*5

AK9*R*1*1*0

SE*8*140343402

GE*1*140343402

IEA*1*140343402

4. Rejected Claim (Real-time 5010): 277 (Unsolicited) Claim Status

However, a claim was rejected, as reported in the U277 that follows the 999. The 277U is returned in response to version claims in batch and real-time claims.

ISA*00* *00* *ZZ*NCTRACKSREL *ZZ*837P *130507*1536*¬*00501*270000088*0*T*:

GS*HN*NCTRACKSREL*DIRECT CONNECT*20130507*153628*270000088*X*005010X212

ST*277*270000088*005010X212

BHT*0010*08*270000088*20130507*153628*DG

HL*1**20*1

NM1*PR*2*NCTRACKS*****PI*NCTRACKS

HL*2*1*21*1

NM1*41*1*DirectConnect*DirectConnect****46*Dire

HL*3*2*19*1

NM1*1P*2*PHYSICIAN*****XX*1972807352

HL*4*3*22*0

NM1*IL*1*LAST*FIRST*M***MI*122582454L

TRN*2*1212

STC*F2:21*20130507**150.00*0*20130507

REF*1K*1312700000880000

REF*EJ*1212

DTP*472*RD8*20130301-20130301

SVC*HC:99215*150.00*.00****1.000

STC*F2:91:82*20130507********F2:145:82

DTP*472*RD8*20130301-20130301

SE*19*270000088

GE*1*270000088

IEA*1*270000088

7.1.5 Acknowledgments for Batch Transactions

Acknowledgments (999) to inbound Eligibility (270), Claim Status Inquiry (276), Enrollment (834), and Claims (837 I, P, D) transactions are generally available within 24 hours.

7.2 REMITTANCE ADVICE

NCTracks produces remittance advices (835) on a weekly processing cycle basis as an acknowledgment to 837 and NCPDP claims submitted. The Checkwrite cycle for NCTracks is published at the following website:

https://medicaid.ncdhhs.gov/

8. Additional Trading Partner Information

8.1 IMPLEMENTATION CHECKLIST

Trading Partners must have a signed and approved Trading Partner Agreement (TPA). Trading Partners submitting inbound transactions must be certified using the NCTracks Trading Partner Testing Portal. For additional checklists, visit the following websites:

http://www.nctracks.nc.gov/

8.2 TRANSMISSION EXAMPLES

Trading Partners should refer to the X12 standards documents and NCTracks transaction companion guides for examples or information regarding control segments and envelopes. The companion guides are available at the following website:

http://www.nctracks.nc.gov/provider/guides/index.html

8.3 TRADING PARTNER AGREEMENT

EDI Trading Partner Agreements ensure the integrity of the electronic transaction process. The Trading Partner Agreement is related to the electronic exchange of information, whether the agreement is an entity or a part of a larger agreement, between each party to the agreement.

For example, a Trading Partner Agreement may specify, among other things, the roles and responsibilities of each party to the agreement in conducting standard transactions.

8.4 FREQUENTLY ASKED QUESTIONS

1. **Who are classified as Trading Partners that are required to be certified in the Trading Partner Testing Portal?**

   Trading Partners who are classified as clearinghouses, billing agents, VANs, and LMEs (DMH) who will be submitting one or more of the following inbound transactions: 837 (I, P, and D), 270, 276, and 834I.

2. **Are providers other than Clearinghouses, Billing Agents, and VANs also required to be certified in the Trading Partner Testing Portal?**

   No, only clearinghouses, billing agents, and VANs who will be submitting claims on behalf of providers will need to be certified in the Trading Partner Testing Portal. However, any individual or organization providers who may be submitting these inbound transactions without using clearinghouses or billing agents should be certified in the Trading Partner Testing Portal.

3. **In which transactions will Trading Partners need to be certified in the Trading Partner Testing Portal?**

   Trading Partners will need to be certified in any of the following transactions that they are planning to submit in NCTracks:

   - 270 – Eligibility
   - 837I – 837 Institutional
   - 837P – 837 Professional
   - 837D – 837 Dental

- 276 – Claims Status
- 834I – Benefit Enrollment and Maintenance

4. Will the NCPDP D.0 transactions be certified through the Trading Partner certification process in the Trading Partner Testing Portal?

No. The switch vendors will be performing the testing of D.0 outside of the Trading Partner Testing Portal; these transactions are not included in the Trading Partner Testing Portal and the Trading Partner certification process.

5. Do Trading Partners need to be certified in both 4010 and 5010 inbound transactions?

Trading partners need to be certified only in 5010 since NCTracks supports only 5010 transactions.

6. Do Trading Partners need to be certified in the Trading Partner Testing Portal to receive outbound transactions such as 835, 820, etc.?

No. However, this information is required during the enrollment process via the Provider portal.

7. Is the Trading Partner certification process dependent on the EVC registration process for Billing Agents?

No. These tasks can run in parallel, and EVC registration is not required to be completed before the Trading Partner certification begins.

8. After Trading Partners are certified, do they need to submit the transactions into NCTracks as part of the certification testing?

No.

9. Can a Trading Partner sign up and be certified in the Trading Partner Testing Portal without an email address?

No. This is a prerequisite for Trading Partners to sign up and be certified in the Trading Partner Testing Portal.

10. How will Trading Partners be invited?

Invites will go out to Trading Partners via email from the Trading Partner Testing Portal. The outreach letter to all Trading Partners will be sent to the mailing address by the State Provider Communications team.

11. Will Trading Partners be trained on the Trading Partner Testing Portal?

No. This is because the Trading Partner Testing Portal is a self-service portal and has Trading Partner Testing Portal user guides that can be used to complete the certification process.

12. Should the TPA be signed before Trading Partners are certified?

Yes. Trading Partners who will be participating in the Trading Partner certification process will electronically sign the TPA in the Trading Partner Testing Portal.

13. How will Trading Partners access the Trading Partner Testing Portal?

After the Trading Partner's contact information is uploaded into the Trading Partner Testing Portal, the Trading Partner will receive a hyperlink, user ID, and password to the Trading Partner Testing Portal.

14. Will Trading Partners receive reminders on the certification process?

Yes. Automatic reminders from the Trading Partner Testing Portal will be sent to the Trading Partner's email address.

15. Will Trading Partners be notified when certified successfully?

Yes; after all the tasks in the Trading Partner Testing Portal are completed successfully, an automatic notification will be sent by the Trading Partner Testing Portal for each program.

16. In which programs will Trading Partners enroll to become certified?

All Trading Partners should be enrolled under all the inbound programs in the Trading Partner Testing Portal. If this information can be easily obtained before the invites from the Trading Partner Testing Portal go out to Trading Partners, then only the selected Trading Partners for each transaction will be notified to become certified in the respective transactions.

17. What are the steps for Trading Partners to become compliance certified?

- Receive the invites from the Trading Partner Testing Portal.
- Update Trading Partner's profile and enroll into the program using the logon and password provided on the invites.
- Sign the TPA manually in the Trading Partner Testing Portal.
- Use the Companion Guide and the guidelines document posted in the Trading Partner Testing Portal.
- Submit test files for the programs in which the Trading Partner is enrolled.
- Log any issues via the Trading Partner Testing Portal, or call or email the CSRA EDI helpdesk.
- Become certified in the Trading Partner Testing Portal using the test files submitted into the portal.
- Fill out surveys sent out through the Trading Partner Testing Portal.

18. Will CSRA provide an EDI helpdesk phone number or email address to receive any issues?

The EDI helpdesk phone number is: 1-800-688-6696, option #1, and the email address is: NCMMIS_EDI_SUPPORT@gdit.com. The subject of the email should be "TRADING PARTNER TESTING" so that it is directed to the correct mailbox folder. This support will be available from 9:00 a.m. to 5:00 p.m. EST.

19. Where will the Companion Guides for all the transactions be posted?

The Companion Guides for all the inbound transactions have been posted at the following location:

http://www.nctracks.nc.gov/provider/guides/index.html

For the Trading Partner certification process, the Companion Guides will be posted in the Trading Partner Testing Portal in the "Reference Material" section of the portal.

20. What if Trading Partners have not completed their certification before Go-Live?

The Inbound X12 transactions submitted by Trading Partners will be rejected by the NCTracks EDI process and will not be processed.

21. Do Trading Partners or individual providers need to be certified or sign the TPA if they submit X12 transactions through the DirectConnect portal?

No.

22. Do the terms ETIN (Electronic Transmitter Identification Number) and TSN (Transaction Supplier Number) mean the same or do they have different meanings?

These terms are synonymous and are used interchangeably in the Connectivity Guide and Companion Guides.

8.5 OTHER RESOURCES

8.5.1 NCTracks Fiscal Agent

Information about a variety of topics essential to NCTracks providers and their Business Associates, including topics such as provider enrollment, training, and establishing and using the various communication channels for exchanging electronic claims and related transactions, is publicly available at:

http://www.nctracks.nc.gov/provider/index.html

8.5.2 Other Useful Websites

- The registry for the NPI (National Provider Identifier) is the National Plan and Provider Enumeration System (NPPES), at:

  http://nppes.cms.hhs.gov/NPPES/Welcome.do
- Other resources pertaining to the National Provider Identifier:

  http://www.cms.hhs.gov/NationalProvIdentStand/
- Implementation Guides and Non-medical code sets are at:

  http://store.x12.org/
- The HIPAA statute, Final Rules, and related NPRMS (Notices of Proposed Rulemaking) are available at:

  http://www.cms.hhs.gov/HIPAAGenInfo/

  http://aspe.hhs.gov/datacncl/adminsim.shtml
- Information from CMS about ICD-9 and ICD-10 codes:

  http://www.cms.hhs.gov/ICD9ProviderDiagnosticCodes/01_overview.asp#TopOfPage

  http://www.cms.hhs.gov/ICD9ProviderDiagnosticCodes/08_ICD10.asp#TopOfPage
- Quarterly updates to the HCPCS code set are available from CMS at:

  http://www.cms.hhs.gov/HCPCSReleaseCodeSets/

  CPT-4, or Level 1 HCPCS, is maintained and licensed by the American Medical Association and is available for purchase in various hardcopy and softcopy formats from a variety of vendors.

- Information at the federal level about Medicaid can be found at: http://www.cms.hhs.gov/home/medicaid.asp
- The CMS online Manuals system includes Transmittals and Program Memoranda at: http://www.cms.hhs.gov/Manuals/
- Place of Service Codes maintained by (CMS) online: http://www.cms.gov/PlaceofServiceCodes/

Appendix A. Ipswitch Tested FTP Clients

A.1 SUPPORTED SECURE FTP/SSH (AND SCP2) CLIENTS

MoveIT DMZ has been tested against and fully supports the following secure FTP clients using FTP over SSH:

- OpenSSH sftp for *nix (free command-line, Unix – including Linux and BSD, password and client key modes)
- OpenSSH for Windows (free command-line, Windows, password and client key modes)
- OpenSSH sftp for Mac (preinstalled command-line, Mac, password and client key modes)
- OpenSSH sftp for z/OS (part of IBM Ported Tools for z/OS, z/OS 1.4+, password and client key modes)
- Putty PSFTP (command-line, Windows, password and client key modes)
- WS_FTP (GUI, Windows, version 7.0 and higher; version 7.62 has a compression-related bug that prevents it from uploading large, highly compressible files)
- BitKinex (GUI, version 2.5 and higher, Windows)
- F-Secure SSH (command-line, 3.2.0 Client for Unix, password and client key modes)
- FileZilla (GUI, Windows)
- SSH Communications SSH Secure Shell FTP (GUI, Windows, password and client key modes; requires setting number of transfers to 1)
- SSH Tectia Connector (Windows)
- SSH Tectia Client (Windows, AIX, HP-UX, Linux, Solaris)
- J2SSH (free Java class – requires Java 1.3+)
- Net:SFTP – Net::SSH::Perl (free Perl module for Unix)
- MacSSH (GUI, Mac, password mode only)
- Fugu (free GUI, Mac, password mode only)
- Cyberduck (free GUI, Mac, password and client key modes)
- Rbrowser (GUI, Mac, password mode only)
- Transmit2 (GUI, Mac, password and client key modes)
- gftp (GUI, Linux, password and client key modes)
- Magnetk LLC sftpdrive (Windows “drive letter”, password mode only)
- South River Technologies "WebDrive” (Windows “drive letter”, password mode only)
- Cyclone Commerce Interchange (Solaris, client key mode only)
- Stairways Software Pty Ltd. “Interarchy” (Mac “local drive” and GUI, password mode only)
- Miklos Szeredi’s “SSH FileSystem,” also known as “SSHFS” (*nix “mount file system” utility, password and client key modes; requires OpenSSH and FUSE)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)

A.2 SUPPORTED SECURE FTP SSL CLIENTS

MoveIT DMZ has been tested against and fully supports the following secure FTP clients using FTP over SSL:

- MoveIT Freely (free command-line)
- MoveIT Buddy (GUI)
- MoveIT Central (w/Admin)
- WS_FTP Professional and WS_FTP Home (GUI, version 7 and higher, Windows) (version 12 and higher)
- General Information – Client Support
- SmartFTP (GUI, version 1.6 and higher, Windows)
- SmartFTP (free GUI, version 1.0 and higher, Windows)
- Cute FTP Pro (GUI, version 1.0 and higher, Windows)
- BitKinex (GUI, version 2.5 and higher, Windows)
- Glub FTP (GUI, Java 2.0 and higher)
- FlashFXP (GUI, version 3.0 and higher)
- IP*Works SSL (API, Windows, version 5.0)
- LFTP (free command-line, Linux, Unix, Solaris, AIX, etc.)
- NetKit (command-line, Linux, Unix, Solaris, etc.)
- SurgeFTP (command-line, FreeBSD, Linux, Macintosh, Windows, Solaris)
- C-Kermit (command-line; v8.0+, AIX, VMS, Linux, Unix, Solaris)
- AS/400 native FTPS client (OS/400 minicomputer)
- z/OS Secure Sockets FTP client (z/OS mainframe)
- TrailBlaxer ZMOD (OS/400 minicomputer)
- NetFinder (GUI, Apple)
- Sterling Commerce (batch, various)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)
- Cleo Lexicom (batch, various)
- bTrade TDAccess (batch, AIX, AS/400, HP-UX, Linux, MVS, Solaris, Windows)
- cURL (command-line, AIX, HP-UX, Linux, QNX, Windows, AmigaOS, BeOS, Solaris, BSD, and more)
- South River Technologies “WebDrive” (Windows “drive letter” – requires passive, implicit, and ‘PROT P’ options)
- Stairways Software Pty Ltd. “Interarchy” (Mac “local drive” and GUI)

Appendix B. Web Interface

B.1 MOVEIT WIZARD INSTALLATION

The first time a user signs on to the NCTracks MFT system, the system will recognize that the MoveIT Upload/Download Wizard is not installed and will navigate the user to a page from which they can install the Wizard or choose to disable it.

B.1.1 Wizard Requirements

The Upload/Download Wizard has two versions: an ActiveX control, which is only usable by Internet Explorer 7.0 or higher running on Windows, and a Java applet, which can be run on most browsers that support Java applets.

The ActiveX version of the Upload/Download Wizard is available only when using Internet Explorer version 7.0 or higher. In addition, Internet Explorer MUST be configured to accept SIGNED ActiveX controls and run JavaScript, and users working with Internet Explorer must manually click a **Yes** button to download/accept/install the Upload/Download Wizard ActiveX control. Under Windows Vista/Windows 7 with IE7 or later, the ActiveX version also requires the user to mark their MoveIT DMZ site as an IE Trusted Site to take full advantage of Wizard capabilities such as multiple-file download.

The Java version of the Upload/Download Wizard requires the Sun Java2 version 1.5 or higher runtime environment. Java applet support MUST be enabled in the browser, as well as JavaScript support. Finally, the user must click the **Yes** or **Always** button when asked whether they wish to trust the Upload/Download Wizard applet. (Warning: the Java version does not currently run under IE7 and above; use the ActiveX version instead.)

B.1.2 Firewall and Proxy Server Issues

Some firewalls or proxy servers block the “Transfer-Encoding: chunked” header used by the Upload Wizard. When the Upload Wizard detects this situation, it reverts to a different upload protocol. (This alternative protocol is not used by default, because it does not allow compression or the creation of .zip files.) If you have software or network devices that block “Transfer-Encoding: chunked” headers, and find that the MoveIT Wizard is not able to detect this, you can force the Upload Wizard to use the alternative protocol by creating a value in the registry of the computer that is running Internet Explorer.

Run RegEdit and navigate to HKEY_CURRENT_USER\Software\Standard Networks\MoveITUploadWizard. (If this key does not exist, create it.) Then create a DWORD value named ForceNonLumpHashMode and give it a value of 1. This will force the Upload Wizard to use the less-efficient but more widely accepted alternative upload protocol.

B.1.3 Internet Explorer

Internet Explorer users will be sent to the ActiveX Wizard Installation page, which gives options to install the ActiveX Wizard, disable it, or disable it and install the Java Wizard.

Exhibit B-1. Wizard Status

If you select “Try to install”, you will be sent to a page that will attempt to download the ActiveX control. This may take several seconds. You may need to alter your browser’s security settings to permit signed ActiveX controls to be installed in order to successfully complete the process.

If you select “Disable”, you will not be prompted to install the ActiveX Wizard again unless you explicitly request it via the Account Options page. If you select “Disable (this session only)”, during the next browser session, a link to install the Wizard will display.

A dialog may appear, stating that installation of an ActiveX control was blocked. Click **OK** on this dialog. Click the (usually yellow) banner at the top of the page to access a popup menu and select the Install ActiveX Control option.

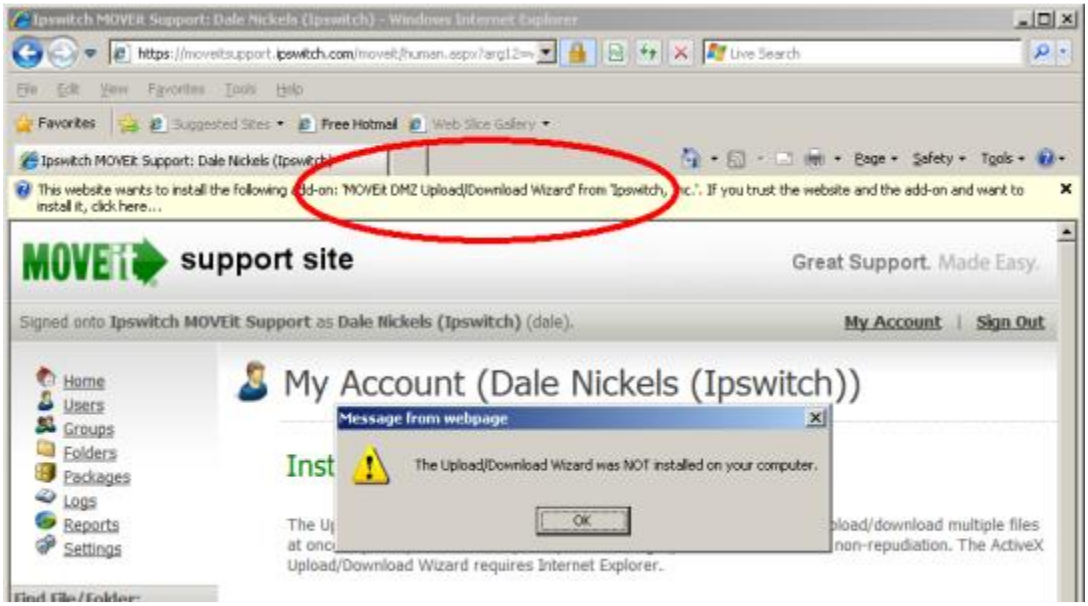


Exhibit B-2. ActiveX Control Block of Wizard Installation

.

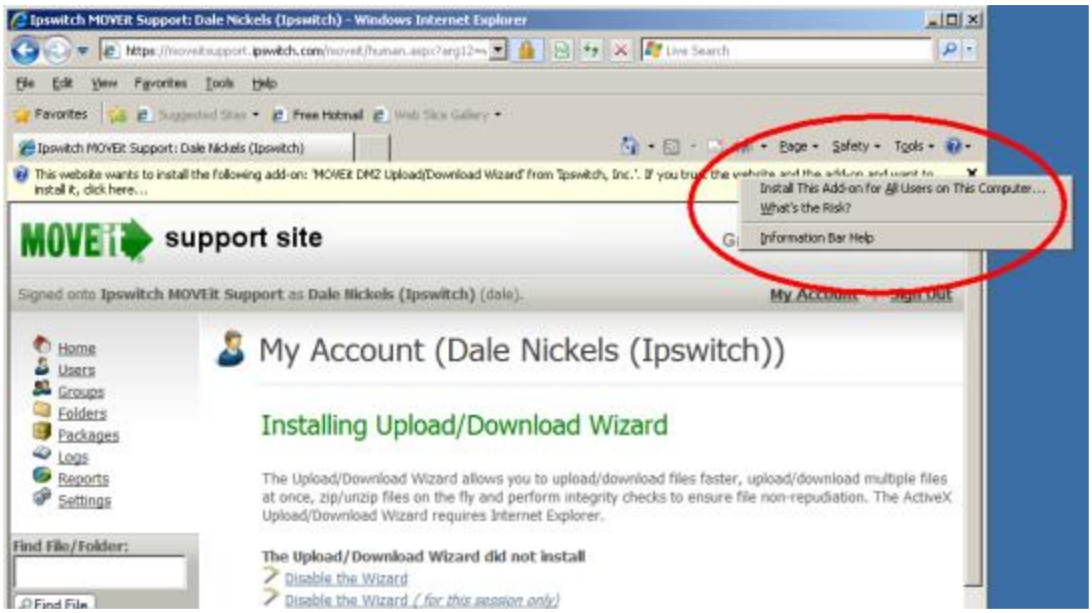


Exhibit B-3. Enable ActiveX Wizard Install

Next, a dialog with a yellow shield will display (this indicates that the Upload/Download Wizard ActiveX control has been cryptographically signed and validated). Click the **Install** button.

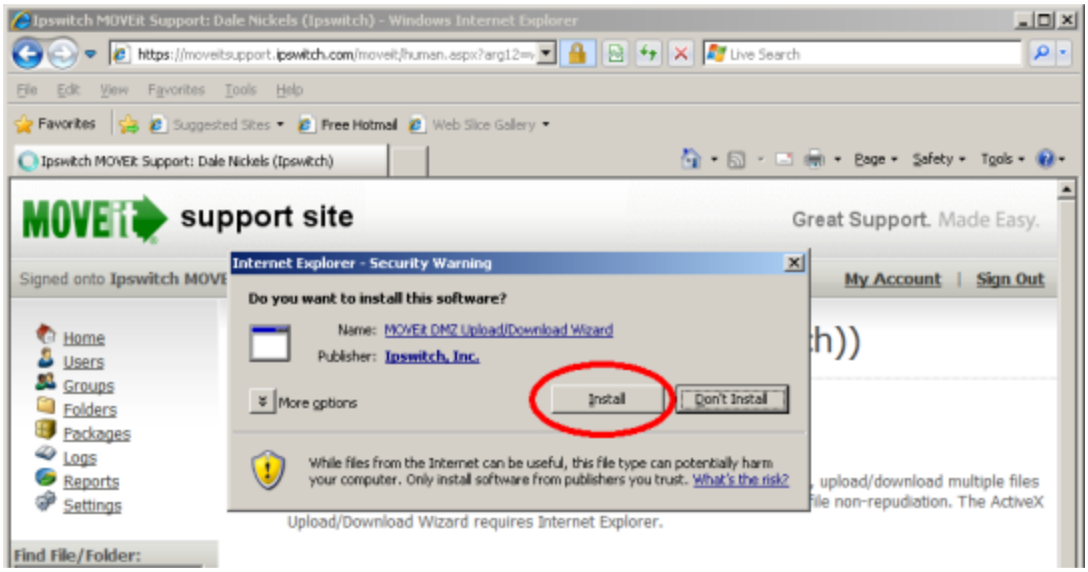


Exhibit B-4. ActiveX Wizard Install

After you complete these extra steps, the Wizard should automatically finish installing.

B.1.4 Internet Explorer 7.0 or Higher

If you are running Internet Explorer 7.0 on Windows Vista, you may need to perform an extra step before you can use all the features of the Wizard, such as the ability to download multiple files at once. This extra step is to add any MoveIT DMZ site with which you communicate into your Internet Explorer list of “Trusted Sites”.

To change your security settings in this way, double-click the “Internet” label (with the globe) at the bottom of your IE browser window.

Exhibit B-5. Access Security Settings

An Internet Security Properties dialog will display. Click the “Trusted sites” icon (the green checkmark) and then click the **Sites** button. A list of existing trusted sites will display, and the NCTracks MFT site will be listed in the “Add this website to the zone” text box. Click the **Add** button to finish trusting the NCTracks MFT site, and use the **Close** and **OK** buttons to dismiss the dialog.

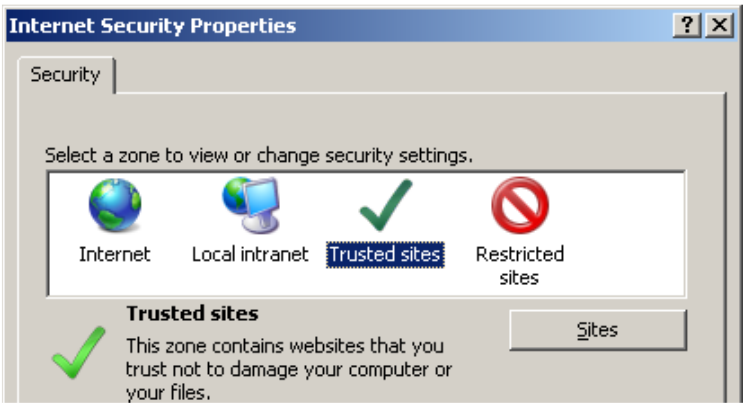


Exhibit B-6. Access Security Trusted Site Settings

When complete, you should see a “Trusted sites” label (with a green checkmark) in place of the “Internet” label (with the globe) at the bottom of your IE browser window.

Exhibit B-7. Confirmed Trusted Site

B.1.5 Other Browsers

The first time a user signs on to the NCTracks MFT site with a browser other than Internet Explorer (e.g., Firefox), the NCTracks MFT site will display a slightly different page with a link to install the Java Upload/Download Wizard. The Java Upload/Download Wizard is a component similar to the ActiveX Wizard, designed for environments that cannot run ActiveX controls. The choices are similar to those for the ActiveX Wizard. If Java is not installed, the user can simply select “Disable” to avoid being prompted to install the Java Wizard in subsequent sessions. Java can be downloaded from the Sun Java website.

B.1.5.1 Install the Java Wizard

Installation of the Java Upload/Download Wizard is generally performed automatically by the browser. You will initially be presented with the following window, asking if you want to run the applet. Click the **Run** button to allow the Java Wizard to run. Selecting the “Always trust content...” checkbox is also recommended.

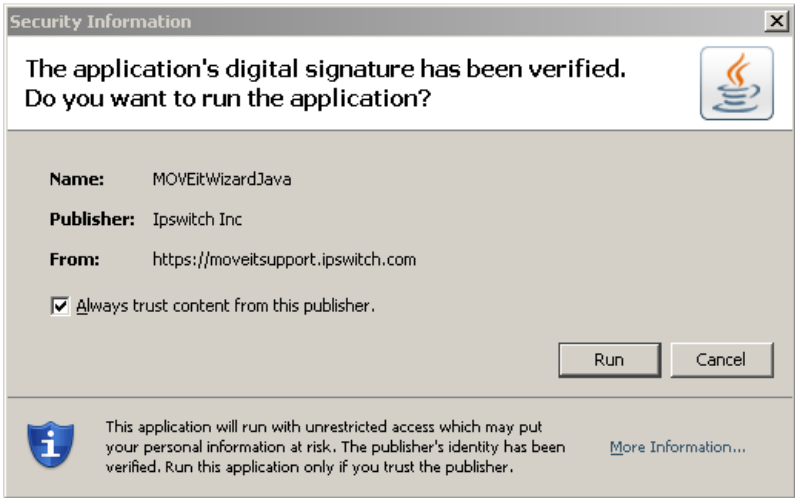


Exhibit B-8. Java Wizard Install

B.2 WEB INTERFACE – UPLOAD/DOWNLOAD WIZARD

The NCTracks MFT MoveIT Upload Wizard gives web users a faster method to transfer files over the web than the usual web transfers performed via the built-in “upload” button, through the use of compression-on-the-fly. The Upload Wizard provides integrity checking; it proves that the file or files that were just uploaded to the server are exactly the same as the files that exist on your local hard drive.

As previously discussed, there are two versions of the Wizard: ActiveX and Java. However, the versions look and behave similarly.

B.2.1 Upload Wizard

1. Start the Upload Wizard.

   The NCTracks MFT MoveIT Upload Wizard will be presented as an option to users who have downloaded the Wizard and enabled it via the My Account page. It will appear on all pages from which uploads are normally permitted. To start the Wizard:

   a. Select the folder into which you want to upload files.
   b. Click the “CLICK HERE to Launch the Upload Wizard...” link.

2. Select the files to be uploaded to the NCTracks MFT MoveIT Upload Wizard.

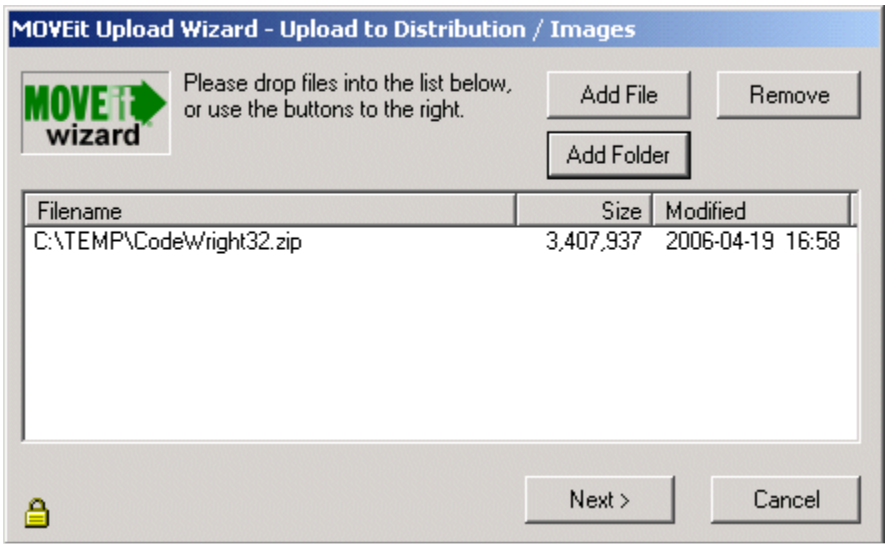


Exhibit B-9. Upload Wizard File Selection

Files to be uploaded can be selected in several different ways:

- Click the **Add File** button and double-click files from the navigation to select individual files.
- Click the **Add File** button and CTRL-click files from the navigation to select multiple files from the same folder.
- Click the **Add Folder** button and select a folder to recursively upload.
- Drag and drop files and/or folders from an Explorer window onto the list of files in the Wizard.

Note: Selected files do not need to be from the same directory — the Upload Wizard can handle files from several different directories and/or drives at the same time.

Click the **Next >** button to continue.

3. Under “Choose Upload Options”, select “Upload files individually”. When this option is selected, each file will be logged on the NCTracks MFT MoveIT Upload Wizard with a separate file ID. Do not compress more than one file in a zip file. Although the NCTracks MFT MoveIT Upload Wizard will allow you to do so, the NCTracks system will reject the file and place it in the “Reject” folder.

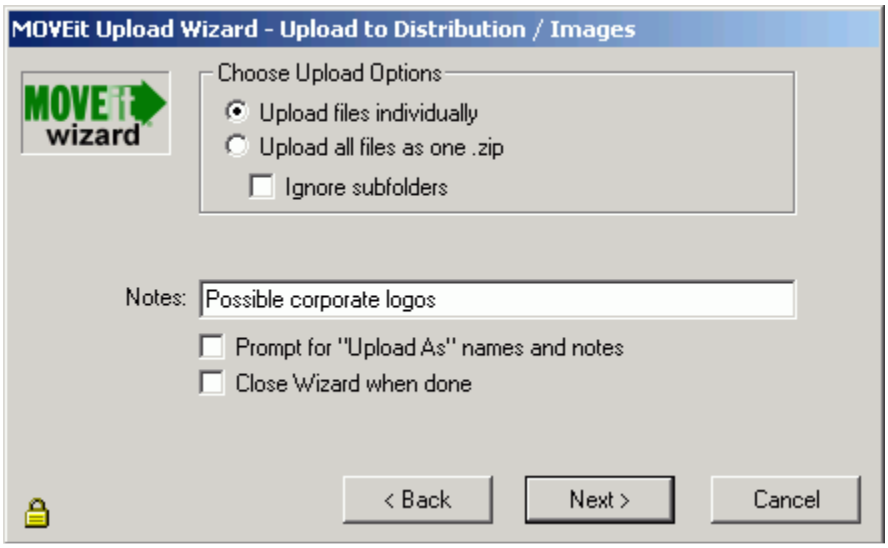


Exhibit B-10. Upload Wizard File Options

Selecting the “Close Wizard when done” checkbox will cause the Wizard to close itself when the transfer is complete.

4. Click the **Next >** button to begin the transfer.
5. When the transfer begins, a progress bar will appear, indicating the portion of the transfer that has been completed. When the transfer is complete, a transfer summary will display.

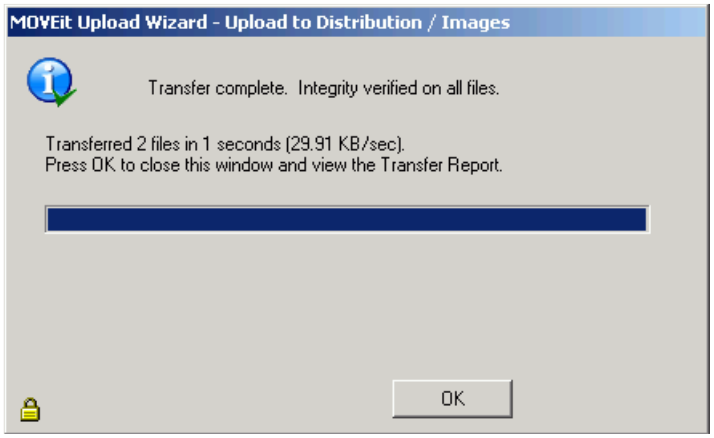


Exhibit B-11. Upload Wizard Progress Bar

B.2.2 Download Wizard

The NCTracks MFT MoveIT Download Wizard gives web users a faster method to transfer files over the web. It also provides the ability for users to download more than one file at a time. In addition, the Download Wizard displays the progress of transfers using a progress bar and provides **Open File**, **Open Folder**, and **Unzip File** buttons when transfers are complete. Finally, the Download Wizard provides integrity checking; it proves that the file or files that were just downloaded from the server are exactly the same as the files that exist on the server.

1. Start the Download Wizard. The NCTracks MFT MoveIT Download Wizard is automatically invoked when you select a Download link. It is also invoked when you click the **Download** button on the File List page.
2. In the first displayed dialog, either Open or Save the file. “Opening” the file means the file will be downloaded to a temporary directory, and after successful completion, the associated application (based on file extension) will be run without any further prompting. “Saving” the file means that you will be prompted for a directory into which the file should be placed. The associated application will not be run automatically.

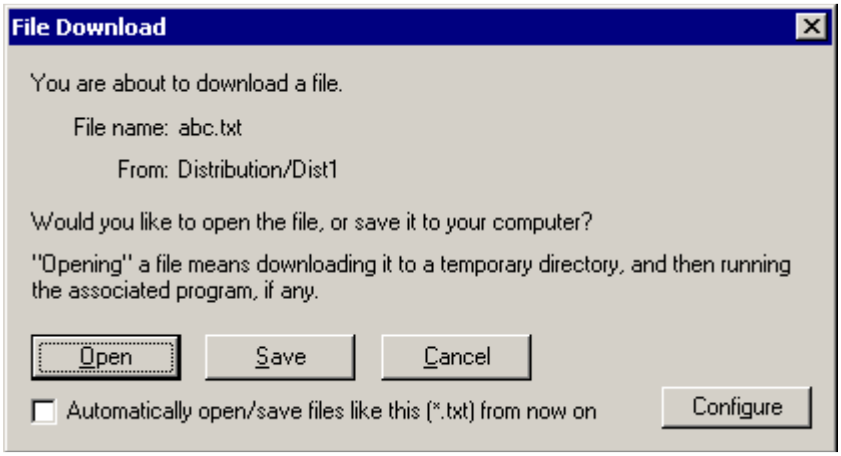


Exhibit B-12. Download Wizard Options

Select the "Automatically open/save files like this from now on” checkbox to prevent this dialog from appearing for files with the same extension in the future. The **Configure** button allows you to configure how files with a given extension are handled. The configuration dialog is also available via the Account Options page.

3. Select the download destination. If you choose Save, the Download Wizard asks for the folder into which the download should be saved as well as the file name to use. If an existing file of the same name already exists in this location, you will be asked if you want to overwrite the existing file.

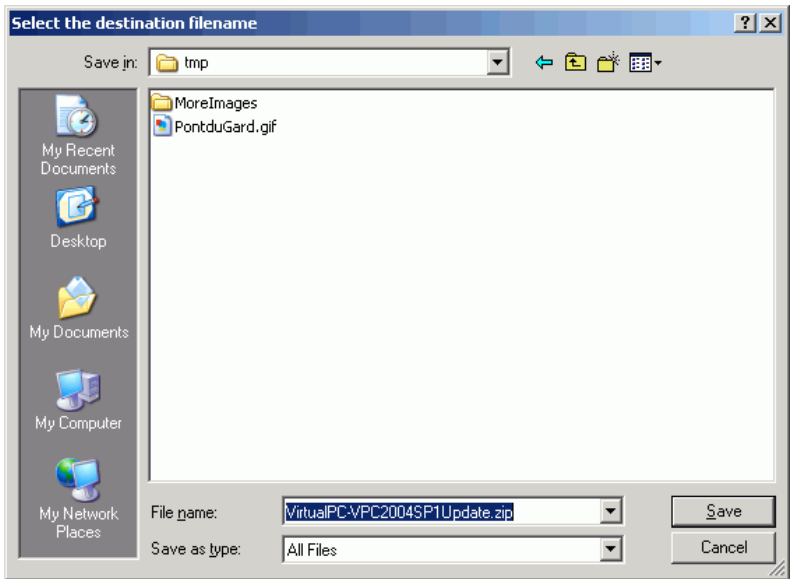


Exhibit B-13. Download Destination Selection

4. When the transfer begins, the Download Wizard will display a progress bar, the size of the download, the amount currently downloaded, an estimate of the transfer speed, and an estimate of the amount of time required to complete the download.

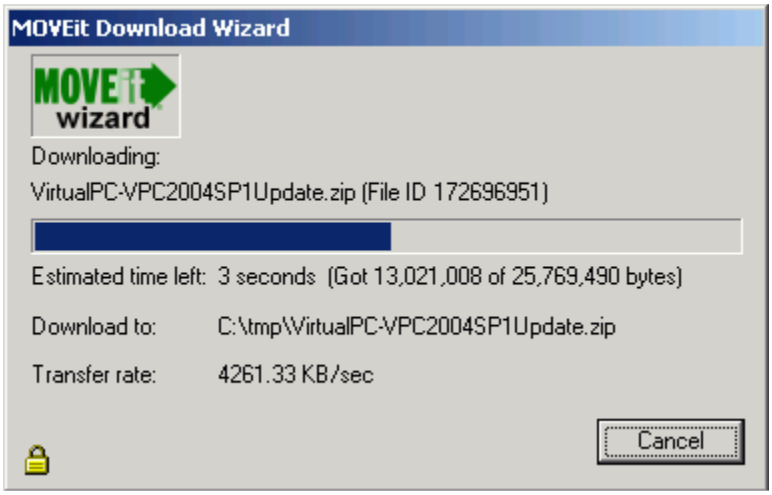


Exhibit B-14. Download Wizard Progress Bar

When the download is complete, the integrity of the downloaded file will be checked. This ensures that the file just downloaded is completely identical to the file on the server. At least three buttons will also be displayed if the transfer was successful:

- **Open** – Opens the file just downloaded, using any file associations currently available.
- **Open Folder** – Browses to the folder into which the file was downloaded.
- **Close** – Closes the Download Wizard immediately.

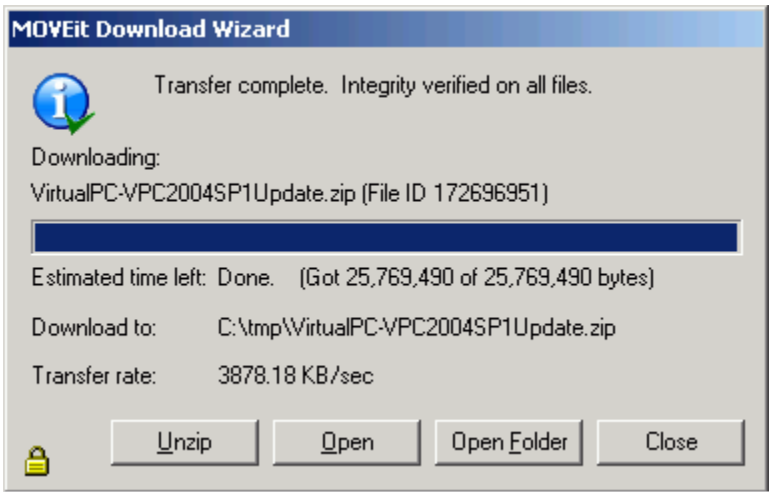


Exhibit B-15. Download Wizard Transfer Complete Options

Appendix C. 270 SOAP and MIME Samples

C.1 270 SOAP BATCH SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
      <wsse:UsernameToken>
         <wsse:Username>tstesgstr</wsse:Username>
         <wsse:Password>valid123</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <cor:COREEnvelopeBatchSubmission>
      <PayloadType>X12_270_Request_005010X279A1</PayloadType>
      <ProcessingMode>Batch</ProcessingMode>
      <PayloadID>f71d4fae-7dec-11d0-a765-00a0c91e6bf1</PayloadID>
      <PayloadLength>467</PayloadLength>
      <TimeStamp>2014-02-03T10:20:34Z</TimeStamp>
      <SenderID>HospitalA</SenderID>
      <ReceiverID>PayerB</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <CheckSum>a5bd32e185234250c719fe1b634fbc01ddf6d696</CheckSum>
      <Payload>cid:Dummy270file-batch1.txt</Payload>
    </cor:COREEnvelopeBatchSubmission>
  </soap:Body>
</soap:Envelope>
```

C.2 270 SOAP REAL-TIME SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
      <wsse:UsernameToken>
         <wsse:Username>tstesgstr</wsse:Username>
         <wsse:Password>valid123</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <cor:COREEnvelopeRealTimeRequest>
      <PayloadType>X12_270_Request_005010X279A1</PayloadType>
      <ProcessingMode>RealTime</ProcessingMode>
      <PayloadID>f71d4fae-7dec-11d0-a765-00a0c91e6bf1</PayloadID>
      <TimeStamp>2014-02-04T10:20:34Z</TimeStamp>
      <SenderID>HospitalA</SenderID>
      <ReceiverID>PayerB</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <Payload><![CDATA[****Valid RealTime ASC X12 transaction embedded here****]]></Payload>
    </cor:COREEnvelopeRealTimeRequest>
  </soap:Body>
</soap:Envelope>
```

C.3 270 MIME BATCH SAMPLE

```
--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

a21d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

tstcaquat2
--XbCY
Content-Disposition: form-data; name="Password"

Test@2014
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="CheckSum"

022bf518a245234c5c23c4351b75df51078c17ea
--XbCY
Content-Disposition: form-data; name="Payload"

[****Valid RealTime ASC X12 transaction embedded here****]
--XbCY--
```

C.4 270 MIME REAL-TIME SAMPLE

Content-Type: multipart/form-data; boundary= XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2014-02-18T10:30:02Z
--XbCY
Content-Disposition: form-data; name="UserName"

NCID
--XbCY
Content-Disposition: form-data; name="Password"

Password
--XbCY
Content-Disposition: form-data; name="SenderID"

SenderID
--XbCY
Content-Disposition: form-data; name="ReceiverID"

NCTracks
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"

Valid Batch ASC X12 transaction embedded here
--XbCY--

Appendix D. 276 SOAP and MIME Samples

D.1 276 SOAP BATCH SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
      <wsse:UsernameToken>
          <wsse:Username>ravindar-reddy</wsse:Username>
            <wsse:Password>valid321</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <cor:COREEnvelopeBatchSubmission>
      <PayloadType>X12_276_Request_005010X212</PayloadType>
      <ProcessingMode>Batch</ProcessingMode>
      <PayloadID>f81d4fae-7dec-11e0-a1b3-00a0d81e1ef7</PayloadID>
      <PayloadLength>467</PayloadLength>
      <TimeStamp>2014-08-13T20:36:32Z</TimeStamp>
      <SenderID>HospitalA</SenderID>
      <ReceiverID>PayerB</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <CheckSum>a5bd32e185234250c719fe1b634fbc01ddf6d696</CheckSum>
      <Payload>cid:Dummy276file-batch.txt</Payload>
    </cor:COREEnvelopeBatchSubmission>
  </soap:Body>
</soap:Envelope>
```

D.2 276 SOAP REAL-TIME SAMPLE

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
  <soapenv:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="true">
      <wsse:UsernameToken>
      <wsse:Username>ravindar-reddy</wsse:Username>
      <wsse:Password>valid321</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <ns1:COREEnvelopeRealTimeRequest xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
      <PayloadType>X12_276_Request_005010X212</PayloadType>
      <ProcessingMode>RealTime</ProcessingMode>
      <PayloadID>59a33e23-990f-4f3d-8dd2-afd329a8f2ae</PayloadID>
      <TimeStamp>2014-08-07T14:53:30Z</TimeStamp>
      <SenderID>DMLR</SenderID>
      <ReceiverID>NCTRACKS</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <Payload><![CDATA[****Valid RealTime ASC X12 transaction embedded here****]]></Payload>
    </ns1:COREEnvelopeRealTimeRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

D.3 276 MIME BATCH SAMPLE

```
--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_276_Request_005010X212
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa7
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

vghantp1
--XbCY
Content-Disposition: form-data; name="Password"

valid121
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="CheckSum"

2ef22f4ced8858f738496ae9a506f3f992ee5863
--XbCY
Content-Disposition: form-data; name="Payload"

****Valid RealTime ASC X12 transaction embedded here****
--XbCY—
```

D.4 276 MIME REAL-TIME SAMPLE

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_276_Request_005010X212
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

vghantp1
--XbCY
Content-Disposition: form-data; name="Password"

valid121
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"

****Valid RealTime ASC X12 transaction embedded here****
--XbCY—

Appendix E. 999 Request SOAP and MIME Batch Samples

E.1 999 REQUEST SOAP BATCH SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
      <wsse:UsernameToken>
        <wsse:Username>ravindar-reddy</wsse:Username>
          <wsse:Password>valid321</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <cor:COREEnvelopeBatchSubmissionAckRetrievalRequest>
      <PayloadType>X12_999_RetrievalRequest_005010X231A1</PayloadType>
      <ProcessingMode>Batch</ProcessingMode>
      <PayloadID>f81d4fae-7dec-11e0-a1b3-00a0d81e1ef7</PayloadID>
      <PayloadLength>467</PayloadLength>
      <TimeStamp>2014-08-03T10:20:34Z</TimeStamp>
      <SenderID>HospitalA</SenderID>
      <ReceiverID>PayerB</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
    </cor:COREEnvelopeBatchSubmissionAckRetrievalRequest>
  </soap:Body>
</soap:Envelope>
```

E.2 999 REQUEST MIME BATCH SAMPLE

Content-Type: multipart/form-data; boundary= XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_999_SubmissionRequest_005010X231A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

a81d4fae-7dec-11d0-a765-00a0d91e6fa7
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2014-02-18T10:30:02Z
--XbCY
Content-Disposition: form-data; name="UserName"

NCID
--XbCY
Content-Disposition: form-data; name="Password"

Password
--XbCY
Content-Disposition: form-data; name="SenderID"

SenderID
--XbCY
Content-Disposition: form-data; name="ReceiverID"

NCTracks
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="CheckSum"

06df47b20dabbf5851f7bd51d4798a056726f3d1
--XbCY
Content-Disposition: form-data; name="Payload"

Valid Batch ASC X12 transaction embedded here
--XbCY—

Appendix F. 835 SOAP and MIME Batch Samples

F.1 835 REQUEST SOAP BATCH SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
      <wsse:UsernameToken>
         <wsse:Username>rsurkanti-dev</wsse:Username>
         <wsse:Password>Ravi-920</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
     <cor:COREEnvelopeBatchResultsRetrievalRequest>
        <PayloadType>X12_835_Request_005010X221A1</PayloadType>
        <ProcessingMode>Batch</ProcessingMode>
        <PayloadID>f71d4fae-7dec-11d0-a765-00a0c91e6b12</PayloadID>
        <!--Optional:-->
        <PayloadLength>467</PayloadLength>
        <TimeStamp>2014-02-03T10:20:34Z</TimeStamp>
        <SenderID>HospitalA</SenderID>
        <ReceiverID>PayerB</ReceiverID>
        <CORERuleVersion>2.2.0</CORERuleVersion>
        <!--Optional:-->
          <CheckSum>a5bd32e185234250c719fe1b634fbc01ddf6d696</CheckSum>
        <!--Optional:-->
<Payload><![CDATA[UFlNVERBVEU6MjAxNC0wNi0xOSxQSUQ6MDEyMzQ1Njc4OSxUU046MTIzNCxGSUxFSUQ6MTQwODQwMDAwMTAwMDIyMEZG]]></Payload>
     </cor:COREEnvelopeBatchResultsRetrievalRequest>
  </soap:Body>
</soap:Envelope>
```

F.2 835 REQUEST MIME BATCH SAMPLE

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_820_Request_005010X218A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fb1
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2014-06-03T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

rsurkanti-dev
--XbCY
Content-Disposition: form-data; name="Password"

Ravi-920
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"

UFlNVERBVEU6MjAxNC0wNi0yNSxQSUQ6NTAyNjQwMzQwMCxUU046MTIzNCxGSUxFSUQ6MTQxO
TAwMDAwMDAwMDkzOEZG
--XbCY--

Appendix G. 820 SOAP and MIME Batch Samples

G.1 820 REQUEST SOAP BATCH SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
      <wsse:UsernameToken>
         <wsse:Username>rsurkanti-dev</wsse:Username>
         <wsse:Password>Ravi-920</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
     <cor:COREEnvelopeBatchResultsRetrievalRequest>
        <PayloadType>Request_File_List_820</PayloadType>
        <ProcessingMode>Batch</ProcessingMode>
        <PayloadID>f71d4fae-7dec-11d0-a765-00a0c91e6b13</PayloadID>
        <!--Optional:-->
        <PayloadLength>467</PayloadLength>
        <TimeStamp>2014-06-03T10:20:34Z</TimeStamp>
        <SenderID>HospitalA</SenderID>
        <ReceiverID>PayerB</ReceiverID>
        <CORERuleVersion>2.2.0</CORERuleVersion>
        <!--Optional:-->
        <Payload><![CDATA[UFlNVERBVEU6MjAxNC0wNi0xOSxQSUQ6MDEyMzQ1Njc4OSxUU046MTIzNA==]]></Payload>
     </cor:COREEnvelopeBatchResultsRetrievalRequest>
  </soap:Body>
</soap:Envelope>
```

G.2 820 REQUEST MIME BATCH SAMPLE

--Xbcy
Content-Disposition: Form-Data; Name="Payloadtype"

X12_820_Request_005010x218a1
--Xbcy
Content-Disposition: Form-Data; Name="Processingmode"

Batch
--Xbcy
Content-Disposition: Form-Data; Name="Payloadid"

F81d4fae-7dec-11d0-A765-00a0d91e6fb1
--Xbcy
Content-Disposition: Form-Data; Name="Timestamp"

2014-06-03t10:20:34z
--Xbcy
Content-Disposition: Form-Data; Name="Username"

Rsurkanti-Dev
--Xbcy
Content-Disposition: Form-Data; Name="Password"

Ravi-920
--Xbcy
Content-Disposition: Form-Data; Name="Senderid"

Hospitala
--Xbcy
Content-Disposition: Form-Data; Name="Receiverid"

Payerb
--Xbcy
Content-Disposition: Form-Data; Name="Coreruleversion"

2.2.0
--Xbcy
Content-Disposition: Form-Data; Name="Payload"

Uflnverbveu6mjaxnc0wni0ynsxqsuq6ntaynjqwmzqwmcxuu046mtiznCxgsuxfsuq6mtqxotawmdawmdawmd
kzoezg
--Xbcy--

Appendix H. 999 Submission SOAP and MIME Samples

H.1 999 SUBMISSION SOAP BATCH SAMPLE

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
  <soap:Header>
  <wsse:Security soap:mustUnderstand="true" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
      <wsse:UsernameToken>
        <wsse:Username>ravindar-reddy</wsse:Username>
        <wsse:Password>valid321</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <cor:COREEnvelopeBatchResultsAckSubmission>
      <PayloadType>X12_999_SubmissionRequest_005010X231A1</PayloadType>
      <ProcessingMode>Batch</ProcessingMode>
      <PayloadID>d32d4fae-7dec-11d0-a765-00a0d91e4bb4</PayloadID>
      <PayloadLength>467</PayloadLength>
      <TimeStamp>2014-08-12T16:49:10Z</TimeStamp>
      <SenderID>HospitalA</SenderID>
      <ReceiverID>PayerB</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <CheckSum>8b2f354e4485c985ba28f35aee921f68bec8e0da</CheckSum>
      <Payload>cid:999BatchFile.X12</Payload>
    </cor:COREEnvelopeBatchResultsAckSubmission>
  </soap:Body>
</soap:Envelope>
```

H.2 999 SUBMISSION MIME BATCH SAMPLE

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_999_SubmissionRequest_005010X231A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"

f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY
Content-Disposition: form-data; name="PayloadLength"

10240
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

ravi-dev
--XbCY
Content-Disposition: form-data; name="Password"

valid321
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.2.0
--XbCY
Content-Disposition: form-data; name="CheckSum"

25a4e9807f1609bf00f25f32a97d7b7ef52870b7
--XbCY
Content-Disposition: form-data; name="Payload"

******Valid RealTime ASC X12 transaction embedded here******
--XbCY

Change Summary

Date	Change	Responsible Party
June 7, 2013	WPDT 01	CSC under the direction of NC DHHS
June 21 2013	Removed references to “real-time submissions for D.0 transactions” under section 4.2.3. Changed the URL in section 4.2.1.5 from “ftp.nctracks.nc.gov” to “ftp2.nctracks.nc.gov” Formatted the payload information on the section 4.2.3. Changed the section “4.2.1.3 File Naming Standards” to give additional details.	CSC under the direction of NC DHHS
March 17, 2014	CAQH-CORE Phase II	CSC under the direction of NC DHHS
September 09, 2014	CAQH-CORE Phase III standards draft template version	CSC under the direction of NC DHHS
November 02, 2014	CAQH-CORE Phase III and MoveIT updates	CSC under the direction of NC DHHS
February 03, 2016	Update to Fiscal Agent name and logo	CSRA under the direction of NC DHHS
March 20, 2017	Update EDI contact information	CSRA under the direction of NC DHHS
October 28, 2018	Updated from Division of Medical Assistance to Division of Health Benefits	CSRA under the direction of NC DHHS
December 15, 2020	Updated MOVEit instructions	CSRA under the direction of NC DHHS
March 3, 2021	Updated EDI Support email address	CSRA under the direction of NC DHHS